Twyford CofE Academies Trust

| | |
|---|---|
| **Document Title** | **Data Protection and Confidentiality Policy** |
| **Committee Responsible for Policy** | **Resources** |
| **Review Frequency** | **Every 3 years** |
| **Last Reviewed** | **November 2020 (updated March 2022)** |
| **Next Review Due** | **November 2023** |
| **Policy Author** | **Richard Lane, Director of Finance & Operations** |

**Assessment of the Impact of a Policy on Equality & Diversity**

| | |
|---|---|
| **Policy:** Data Protection and Confidentiality Policy | |
| **Impact assessed by:** | **Date:** 18/3/2022 |
| **1. What is the potential for this policy impacting a person or group with a protected characteristic differently (favourably or unfavourably) from everyone else?**<br><br>The policy may have greater application to people in protected groups as sensitive information about their protected characteristics (e.g. disability, sexuality) may be held. The policy is therefore part of the Trust's system for ensuring these groups do not receive more or less favourable treatment. | |
| **2. How would this be evidenced?**<br><br>By monitoring the volume of records held and events relating to those records for the different protected groups, so far as this is practical. | |
| **3. Is there evidence that the operation of the current policy might impact a person or group with a protected characteristic differently from everyone else?**<br><br>NO | |
| **4. If the answer to 3 is 'Yes', please provide details and evidence.** | |
| **5. How might the new policy change this?** | |
| **6. Are there any other changes to the policy which might impact a group with a protected characteristic differently from everyone else?**<br><br>NO | |
| **7. If the answer to 6 is 'Yes', please provide details and evidence.** | |

| |
|---|
| **8. Policies are required to reduce or eliminate inequality and disadvantage and promote diversity. Does this assessment indicate that the Policy passes or fails this test?**<br>PASS |

# Data Protection and Confidentiality Policy

Twyford CofE Academies Trust and its schools ("The Trust") collect and use personal information about staff, pupils, parents and other individuals with whom it comes into contact. This information is gathered in order to enable it to provide education and other associated functions. In addition, there are legal requirements to collect and use information to ensure that the school complies with its statutory obligations.

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with data protection legislation. It is based on guidance published by the Information Commissioner's Office (ICO) on the Data Protection Act 2018, the General Data Protection Regulation (EU 2016/679) (GDPR) and GDPR (UK). Additionally, it meets the requirements of the Protection of Freedoms Act 2012, ICO's code of practice in relation to CCTV usage, and the DBS Code of Practice in relation to handling sensitive information. This policy complies with the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files, electronically or is a disclosure made to a member of staff. It should be read in conjunction with the Trust's Data and Document Retention Policy.

## 1 Policy Statement

The Trust is fully committed to compliance with the requirements of data protection legislation, the Children's Act 2004 and other relevant Acts of parliament or regulations insofar as they create duties on Data Controllers and Data Processors (the Twyford Trust is both) concerning the use of personal information. Accordingly, the Trust is registered as a Data Controller with the Information Commissioner's Office. The Trust will therefore follow procedures that aim to ensure that all employees, contractors, agents, consultants, or partners who have access to any personal data held by or on behalf of the Trust, are fully aware of and abide by their legal duties and responsibilities. Failure to comply may lead to disciplinary action and/or prosecution.

### *1.1 Types of Personal Information*

Data protection legislation makes a distinction between personal data and "sensitive" personal data. Personal data is defined as data relating to a living individual who can be identified from:

- That data;
- That data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Data protection legislation now explicitly includes information such as IP addresses.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health condition;
- Genetic information;
- Sexual life;

Under the GDPR, sensitive personal data no longer includes criminal proceedings or convictions, but similar controls and safeguards are required for the handling of this type of information.

Bank and financial details are also highly sensitive.

### *1.2 The Principles of Data Protection*

The Data Protection Act stipulates that anyone handling personal information must comply with six principles of good practice. These principles are legally enforceable. The Principles require that personal information:

1. Shall be processed fairly and lawfully and in a transparent manner in relation to individuals;
2. Shall be collected for specified, explicit and legitimate purposes and shall not be further processed in a manner that is incompatible with those purposes. Further processing for archiving, research or statistical purposes shall not be considered incompatible with the initial purposes;
3. Shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date. Every reasonable step must be taken to ensure that personal information which is inaccurate, having regard to the purposes for which it is processed, is erased or corrected without delay;
5. Shall be 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;
6. Shall be 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;

Furthermore data protection legislation requires that the controller shall be accountable for, and be able to demonstrate, compliance with the principles.

### *1.3 Legal Basis for Processing Personal Information*

Data protection legislation requires that Controllers are explicit about the legal basis for processing personal information. In the case of the Trust, much of the personal

information we hold is to carry out a task in the public interest (education) and to meet a legal obligation. However, some information is held to enable the discharge of contractual obligations. Where personal data is processed for reasons not covered by these justifications, consent of the data subjects is required (by means of either a paper or online consent form). For pupils under 13, the consent of a parent is always required. Pupils aged 13 and over are normally considered competent to provide their own consent. Privacy notices setting out the bases for holding the personal information of pupils, parents, staff and trustees/governors are attached as Appendices A-D.

## 2 Handling of Personal Information

### *2.1 Data Collection and Disclosures*

Only relevant personal data may be collected and the person from whom it is collected will be informed why the data is being collected, of the data's intended use and any possible disclosures or sharing of the information that may be made.

In order to ensure compliance and the security of personal information as it is collected,

- Staff working with personal data on a PC should ensure that the screen cannot be seen by someone who should not have access to the data.
- PCs should be set up with a password protected screensaver where this doesn't interfere with other uses such as presentations/use of an interactive whiteboard etc.
- All forms and questionnaires requiring people to fill in personal information must include a privacy notice which explains who will use the information and for what purpose (see appendices A and D) and may also require a consent form if the Trust is not legally required to collect it.
- Website forms inviting people to submit personal information must always comply with appropriate security protocols (SSL).
- CCTV will only be used to monitor external doors, entrance lobbies and locations where there is a high risk of break-in, theft or pupil misbehaviour.

Individuals may disclose sensitive personal information to Trust staff and staff will need to decide whether to keep this information confidential or pass it on to other staff or other agencies.

There are limits to confidentiality and staff should make clear when they become aware that a conversation may lead to a disclosure of sensitive personal information that there are limits to confidentiality. These limits relate to ensuring children's safety and well-being. A pupil will be informed when a confidence has to be broken for this reason and will be encouraged to do this for themselves whenever this is possible. This also applies to parents disclosing information in confidence.

Confidential information is:

- Personal information of a private or sensitive nature

- Information that is not already lawfully in the public domain or readily available from another public source
- Information that has been shared in circumstances where the person giving information could reasonably expect that it would not be shared with others.

Different levels of confidentiality are appropriate for different circumstances. Detailed guidelines are attached as Appendix E.

### *2.2 Transmission and Carriage of Personal Information*

It is not normally appropriate to include personal information or an opinion about someone in an email. Great care should be exercised when transmitting/sending files containing personal data about more than one person through the internet, by post or some other means to avoid accidental disclosure. Only the following methods of transmission/carriage are permitted:

- Files being shared with the Local Authority, DFE or other schools must use an approved, secure method of transmission such as S2S with encryption or Switch/Egress. Detailed guidance on secure methods for transferring files are found here: *https://www.egfl.org.uk/finance-and-data/data-collection/secure-access-sa* - For other purposes, a file can be converted into an encrypted zip or PDF file. Small files of less than 100 records can then be emailed. Larger files or files containing sensitive information should then be written to a CD and sent by courier. The password for encrypted files should be telephoned through - not put on an email.
- All sent/transmitted files should be stripped of all unnecessary information. For example, a surname may not be required if the pupil reference number is included.
- Transmission of personal data to another Trust email account, provided the data is needed by the recipient for a legitimate purpose, is secure and acceptable.
- It is not permitted to send printouts of databases of personal records through the post or by courier.
- Personal information for up to 10 people may be conveyed by phone or faxed, although care should be taken to ensure that sensitive information is not left on a fax machine or in a tray which is accessible to people who should not see it.
- Forms containing sensitive personal information for up to 10 individuals can be posted using recorded delivery. Forms for more than 10 people should be hand delivered or conveyed by courier. The sender of the information is responsible for ensuring that it has been received by the receiver.
- Documents containing personal information conveyed by internal post or put into the pigeonhole of another member of staff must be put in an envelope and marked confidential. Post rooms or other rooms with pigeonholes must be kept secure and only accessible to authorised staff.

### *2.3 Storage, Retention and Disposal of Personal Information*

Personal information must be kept securely, to minimise the risk of accidental disclosure, and for no longer than is required to meet the Trust's purposes.

- Personal information in paper form should only be held in approved, secure locations. These locations must be locked to a standard approved by insurers and the files held in a locked cupboard, when not in use. One locked door is sufficient for files held in an archive cupboard which is only occasionally accessed.
- Personal information about members of staff in paper form is only allowed to be held within the HR office or their archives in locked filing cabinets. Managers should not hold their own records on staff except the minimum of day-to-day records which should be held for no more than 1 year.
- Personal information about pupils in paper form is only allowed to be held within designated staff offices, admin. offices or their archives in locked filing cabinets. Information about no more than 30 pupils is only allowed to be taken off-site for day-to-day processing (such as marking or assessing). Storage of sensitive personal information about students off-site is not permitted.
- Paper documents containing personal information should never be left out or on a notice board in view of cleaners or other visitors to offices.
- Staff are not permitted to store personal data in electronic form on any media other than in authorised installations such as SIMS, the payroll system or network filing system. Personal data must not be stored on a PC's C drive or My Documents folder. Neither should it be stored on floppy disks, CDs, memory sticks, laptops or other portable memory devices. The minimum of contact details for no more than 50 individuals may be held on mobile phones.
- CCTV recordings are normally held in a secure location for no longer than 6 months unless it is evidence for an incident.
- Detailed information about pupils should not normally be retained for more than 6 years after the last contact/transaction. However, data about admissions and qualifications may be held for up to 25 years in order to respond to subject access requests. The Trust is required to hold some information about staff in perpetuity. Paper records of personal data which are no longer needed must be shredded. It is not permitted for these records to be put in waste bins without being shredded. More detail about retention of data is found in the Data and Document Retention Policy.
- Publications containing photos and other personal information will only remain on websites for as long as is stated in the Data and Document Retention Policy.

### *2.4 Processing of Personal Information*

Personal Information will only be processed for the purpose for which it was collected and will not be used for incompatible purposes without the consent of the data subject. The person about whom the data is held has a number of rights concerning their personal information:

- The right to be informed. 'Fair processing information' must be provided when the data is first obtained, typically through a privacy notice (see appendices A-D).
- The right of access. Requests for copies of personal information held must be complied with without a charge, normally within 1 month, unless the requests are unfounded, excessive or repetitive. Refer to appendix G for more details about responding to a subject access request.
- The right to rectification. Inaccurate data must be corrected and if they have been passed on to third parties then there is a duty to inform the third party and the data subject about the correction.
- The right to erasure. When the data is no longer required for the purpose it was collected then it must be deleted. Third parties with whom data has been shared must be informed to delete this data.
- The right to restrict processing. In some circumstances, data subjects may require use of their data to be restricted – when there is a dispute about its accuracy, for example.
- The right to data portability. In some circumstances (usually where data is held for contractual purposes), data subjects can require their data to be transferred (to a new supplier, for example) in a portable format.
- The right to object. Data subjects can object to their data being used (for marketing, research or public interest purposes, for example).
- Rights in relation to automated decision making and profiling. Subjects can ask for automated decisions to be checked and/or explained.

### *2.5 Disclosure to Third Parties and Data Sharing*

Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given.

- If a request is made for personal data to be disclosed it is the responsibility of the member of staff to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known personally, proof of identity should be requested. If the person is from a partner agency then it is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimised. Requests should normally be put in writing (email is OK).
- Requests from parents/carers or students for printed lists of the names of students in particular groups, which are frequently sought at Christmas, should be politely refused as permission would be needed from all the data subjects contained in the list. (Note: A suggestion that the child makes a list of names when all the students are present in class will resolve the problem.)
- Personal data will not be used in newsletters, websites or other media without the consent of the data subject. It is the Trust's policy not to associate names of individuals with photographs in published material (except key senior staff).

- Routine consent issues will be incorporated into the Trust's student data collection sheets, to avoid the need for frequent, similar requests for consent being made. Data collection forms will invite separate consent for the use of photographs in different types of publications and biometric data and make it clear that this consent is optional and may be withdrawn at any time.
- All disclosures/subject access requests must be logged with the Data Team and the authority letter filed with it and cross-referenced to the log.

Personal Information is routinely shared with other agencies – such as the local authority and the DFE. Guidelines concerning data sharing are found in appendix F. Data sharing agreements should be in place with all agencies or other organisations receiving personal information from the Trust. A model document is found in appendix H. Compliance with this policy must be a condition of all contracts with organisations processing or storing personal information on behalf of the Trust. Formal agreements/checks are also required with suppliers of software and/or cloud storage providers to ensure compliance with data protection requirements. Guidance on requirements and links to checklists for major suppliers are found here:

*https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644845/Cloud-services-software-31.pdf*

Additional safeguards need to be in place if information is to be transferred to a non-EU country.

It is the Trust's policy to activate automatic screen lock on devices providing access to personal data records to prevent unauthorised access to those records. The Technical Services Manager is responsible for ensuring this is implemented.

### *2.6 Subject Access Requests*

If the Trust receives a request either verbally or in writing from a data subject, asking to see any or all personal data that the Trust holds about them this will be treated as a legitimate Subject Access Request and the Trust will respond within the required 1 month deadline.

All subject access requests must be directed to the Trust Data Team in the first instance.

Requests to view or have copies of personal data will be dealt with wherever possible at a mutually convenient time.

A detailed procedure for handling subject access requests is attached as Appendix G.

## 3 Roles, Responsibilities and Accountability

Data protection legislation creates additional obligations on Data Controllers with more than 250 employees (such as the Twyford Trust) concerning accountability and governance of personal information. The Trust is required to keep a Record of Processing activities, covering:

- Name and details of your organisation (and where applicable, of other controllers, your representative and data protection officer).

- Purposes of the processing.
- Description of the categories of individuals and categories of personal data.
- Categories of recipients of personal data.
- Details of transfers to third countries including documentation of the transfer mechanism safeguards in place.
- Retention schedules.
- Description of technical and organisational security measures.

Furthermore, Privacy Impact Assessments (PIAs) must be completed whenever new technologies are being introduced and processing is likely to result in a high risk to the rights and freedoms of individuals. A template PIA is found in appendix I.

The Trust is also required to appoint a Data Protection Officer (DPO) whose role is to:

- To inform and advise the organisation and its employees about their obligations to comply with data protection laws.
- To monitor compliance with data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

The DPO role can be part of another role or contracted out. If it is an internal role then there should not be a conflict of interest with other responsibilities.

The Trust has appointed the London Diocesan Board for Schools (LDBS) to carry out the role of DPO. The Director of Finance & Operations will be data protection lead within the Trust and will assist the LDBS as required and will review and renew the Trust's Data Protection Registration annually and review this policy every three years.

All staff, contractors and partners are expected to comply with this policy. Staff, parents or pupils who consider that the policy has not been followed in respect of personal data should raise the matter with the Trust's DPO in the first instance or may make a formal complaint using the complaints procedure.

All breaches or near-breaches of this policy and guidelines must be reported to the Director of Finance & Operations as soon as possible.

Breaches likely to result in a risk to the rights and freedoms of individuals must be reported by the DPO to the Information Commissioner within 72 hours of coming to light. Breaches representing a high risk to the rights and freedoms of individuals must be reported to the individuals affected. Failure to comply with these requirements can result in large fines.

Queries relating to these guidelines should be addressed to the Director of Finance & Operations.

The roles and responsibilities for implementing this policy are summarised as follows:

The Trust Board of Directors

- Has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations;
- Approves data protection policies;
- Receives regular reports on data protection activities;
- Keeps up to date on developments in data protection law and practice.

The Data Protection Officer (Claire Mehegan, claire.mehegan@london.anglican.org)

- Provides specialist, independent advice to the Trust on data protection issues;
- Is responsible for reviewing the Trust's data protection policies annually;
- Is responsible for overseeing compliance with data protection law;
- Regularly reports on compliance to the Trust Board of Directors;
- Is the named point of contact for data subjects and for the Information Commissioner's Office.

The Trust Data Protection Lead (Richard Lane, Director of Finance & Operations, rlane@twyfordacademies.org.uk)

- Acts as the representative of the Trust (the Data Controller) on a day-to-day basis;
- Ensures that Trust staff are aware of their data protection responsibilities, including the requirement to maintain and Record of Processing and Privacy Impact Assessments, where relevant to the role;
- Facilitates the work of the Data Protection Officer and consults her concerning data breaches and any other matters requiring specialist advice.

All Staff

- Undertaking annual refresher training on the essentials of data protection compliance and familiarity with this policy;
- Handling all personal information in their day-to-day work in accordance with this training;
- Promptly reporting any data breach that may occur;
- Responding to all subject access requests in accordance with this policy.

## Appendix A: Privacy Notice – Pupils/Parents

How we use pupil and parent/carer information

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use pupil & parent/carer personal data.

We, Twyford Church of England Academies Trust are the 'Data controller' for the purposes of data protection law.

We have appointed Grow Education Partners Ltd as our data protection officer (DPO) and the responsible contact is Claire Mehegan (see 'Contact us' below).

In this privacy notice all references to 'you / your' include both the pupil and the pupil's parents, both individually and collectively, unless otherwise specified.

### 1 The personal data we collect and hold

Personal data that we may collect, use, store, and share (when appropriate) about pupils & parents/carers includes, but is not limited to:

- Personal Information (such as name, date of birth, unique pupil number)
- Contact details and preferences (such as telephone number, email address, postal address, for you and your emergency contacts)
- Assessment information (such as data scores, tracking, and internal/external testing)
- Protected characteristics, (such as ethnic background, religion or belief)
- Special educational needs information (such as EHCP's, statements, applications for support, care or support plans)
- Exclusion information
- Relevant medical information (such as NHS information, health checks, physical and mental health care, immunisation status and allergies and medical conditions, including physical and mental health)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs (such as for internal safeguarding & security purposes, school newsletters, media and promotional purposes).
- Closed-circuit television (CCTV) images captured in school
- Data about your use of the school's information and communications systems
- Payment and banking details where required.

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education ("DfE").

A full breakdown of the information we collect on pupils can be requested by contacting Richard Lane, Director of Finance & Operations (email rlane@twyfordacademies.org.uk, phone 020 3301 3189).

## 2 Why we collect and use this information

The purpose of collecting and processing this data includes but is not limited to:

- Contacting you in relation to your child or to inform you about School events and updates
- Supporting pupil learning
- Monitoring and reporting on pupil progress

Providing appropriate pastoral care

- Protecting pupil welfare and safeguarding
- Assessing the quality of our services

Administering admissions waiting lists

- Carrying out research
- Complying with the law regarding data sharing
- Adhering to the statutory duties placed upon us by the Department for Education.

## 3 The lawful basis on which we use this information

This section contains information about the legal basis that we are relying on when handling your information. These are defined under data protection legislation and for personally identifiably information are:

- You have given consent for one or more specific purposes
- Processing is necessary to comply with the school's legal obligations
- Processing is necessary to protect your vital interests
- Processing is necessary for tasks in the public interest or exercise of authority vested in the controller (the provision of education)
- Processing is necessary for the school's legitimate interests or the legitimate interests of a third party.

When we process special category information, which is deemed to be more sensitive, the following lawful basis are used:

- You have given explicit consent
- It is necessary to fulfil the school's obligations or your obligations
- It is necessary to protect your vital interests
- Processing is carried out by a foundation or not-for-profit organisation (includes religious, political or philosophical organisations and trade unions)
- Reasons of public interest in the area of public health.

An example of how we use the information you provide is:

The submission of the school census returns, including a set of named pupil records, is a statutory requirement on schools under Section 537A of the Education Act 1996.
Putting the school census on a statutory basis:

- means that schools do not need to obtain parental or pupil consent to the provision of information
- ensures schools are protected from any legal challenge that they are breaching a duty of confidence to pupils
- helps to ensure that returns are completed by schools.

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn.

## 4 Collecting pupil information

While the majority of information we collect about pupils & parents/carers is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

## 5 Storing pupil data

We keep your information for as long as we need to in order to educate and look after our pupils.

The majority of this will be stored in the pupil file and this file will follow the pupil whenever they move schools and will be retained by the last school the pupil attends.

Where we are legally required or have a lawful basis to do so we will keep some information after your child has left the School. This will be retained in line with our Data Retention Schedule, a copy of which can be requested by contacting Richard Lane, Director of Finance & Operations (email rlane@twyfordacademies.org.uk, phone 020 3301 3180)

To protect your data, we have data protection policies and procedures in place, including strong organisational and technical measures, which are regularly reviewed. Further information can be found in our Data Protection and Confidentiality Policy or upon request.

## 6 Data Sharing

In order for us to legally, effectively and efficiently function we are required to share data with appropriate third parties, including but not limited to:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education- to meet our legal obligations to share certain information.
- The pupil's family and representatives- such as in the event of an emergency
- Educators and examining bodies- such as ensuring we adhere to examining regulations to guarantee the validity of examinations

- Ofsted- during the course of a school inspection
- Suppliers and service providers – to enable them to provide the service we have contracted them for

Central and local government

- Our auditors- to ensure compliance with our legal obligations
- Health authorities (NHS) - to ensure the wellbeing of pupils
- Security organisations to create a secure workplace for all staff
- Health and social welfare organisations
- Professional advisers and consultants - for us to develop our services and best provide our public service

Charities and voluntary organisations

- Police forces, courts, tribunals, security services - to create a secure workplace for all at the school.
- Professional bodies
- Schools that the pupils attend after leaving us.

## 7 Transferring data internationally

We may send your information to other countries where:

- we or a company we work with store information on computer servers based overseas; or
- we communicate with you when you are overseas.

We conduct due diligence on the companies we share data with and note whether they process data in the UK, EEA (which means the European Union, Liechtenstein, Norway and Iceland) or outside of the EEA.

The UK and countries in the EEA are obliged to adhere to the requirements of the GDPR and have equivalent legislation which confer the same level of protection to your personal data.

For organisations who process data outside the UK and EEA we will assess the circumstances of how this occurs and ensure there is no undue risk.

Additionally, we will assess if there are adequate legal provisions in place to transfer data outside of the UK.

## 8 Why we share information

In order to successfully perform our key functions, we need to share personal data with organisations. For example, we share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

## 9 Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example, via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

## 10 Youth support services

### Pupils aged 13+:

Once our pupils reach the age of 13, we also pass basic pupil information (name, address and date of birth) to our local authority and /or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers.

Any additional information is provided only with opt-in consent from the parent or carer.

This right is transferred to the child / pupil once he/she reaches the age 16.

### Pupils aged 16+:

We will also share basic information about pupils aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers.

For more information about services for young people, please visit our local authority website.

## 11 The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance.

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data.

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

## 12 Data Protection Rights

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them.

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- NOT provide information where it compromises the privacy of others
- Give you a copy of the information in an intelligible form.

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

In most cases, we will respond to subject access requests within 1 month, as required under data protection legislation However, we are able to extend this period by up to 2 months for complex requests or exceptional circumstances.

Your Other Rights regarding your Data:

- Withdraw your consent to processing at any time (This only relates to data for which the school relies on consent as a lawful basis for processing)
- Ask us to rectify, erase or restrict processing of your personal data, or object to the processing of it in certain circumstances and where sufficient supporting evidence is supplied
- Prevent the use of your personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest, official authority or legitimate interests
- Request a copy of agreements under which your personal data is transferred outside of the United Kingdom.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect you)
- Request a cease to any processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Submit a complaint to the ICO
- Ask for your personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Parents/carers also have a legal right to access to their child's educational record.

If you would like to exercise any of the rights or requests listed above, please contact Richard Lane, Director of Finance & Operations (email: rlane@twyfordacademies.org.uk, phone: 020 3301 3189, address: Twyford C of E Academies Trust, Twyford Crescent, London W3 9PP).

The School will comply with the Data Protection legislation in regard to dealing with all data requests submitted in any format, although individuals are asked to preferably submit their request in written format to assist with comprehension.

We reserve the right to verify the requesters identification by asking for Photo ID. If this proves insufficient then further ID may be required.

## 13 Data Protection Breaches

If you suspect that your or someone else's data has been subject to unauthorised or unlawful processing, accidental loss, destruction or damage, we ask that you Richard Lane, Director of Finance & Operations (email: rlane@twyfordacademies.org.uk, phone: 020 3301 3189) and advise us without undue delay.

## 14 Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our independent data protection officer Claire Mehegan at the London Diocesan Board for Schools (claire.mehegan@london.anglican.org).

Alternatively, you can refer a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

## 15 Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact either our School Data Protection Lead, Richard Lane, Director of Finance & Operations (email: rlane@twyfordacademies.org.uk, phone: 020 3301 3189) or our independent Data Protection Officer, Claire Mehegan at the London Diocesan Board for Schools (claire.mehegan@london.anglican.org).

## Appendix B: Privacy Notice – Staff

### How we use staff information

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school.

Twyford Church of England Academies Trust, ("the Trust"/"the School") is the 'Data controller' for the purposes of data protection law.

We have appointed Grow Education Partners Ltd as our data protection officer (DPO) and the responsible contact is Claire Mehegan (see 'Contact us' below).

### 1 The personal data we hold.

Personal data that we may collect, use, store, and share (when appropriate) about those we employ or otherwise engage to work at our school includes, but is not restricted to:

- Personal Information (such as name, date of birth, national insurance number, next of kin, dependents, marital status)
- Contact details (such as telephone number, email address, postal address, for you and your emergency contacts)
- Protected characteristics (such as trade union membership, nationality, language, ethnic origin, sexual orientation and religion or belief, where this has been provided)
- Relevant medical information (such as physical or mental health conditions, including for any disabilities for which the organisation needs to make any reasonable adjustments to fulfil its duty of care)
- Information about your renumeration (such as salary, annual leave, pension, bank details, payroll records, tax status and benefits information)
- Information about your criminal records
- Recruitment information, (such as copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process)
- Qualifications and employment records (such as work history, job titles, working hours, training records and professional memberships)
- Assessments of your performance (such as appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence)
- Outcomes of any disciplinary and/or grievance procedures, including any warnings issued to you and related correspondence
- Details of periods of absence (such as holiday, sickness, family leave, sabbatical, including the reasons for the leave)

- Photographs (for internal safeguarding & security purposes, school newsletters, media, and promotional purposes)
- Closed-circuit television (CCTV) footage
- Data about your use of the school's information and communications system.

We may also hold personal data about you from third parties, such as references supplied by former employers, information provided during the completion of our pre-employment checks, and from the Disclosure & Barring Service, in order to comply with our legal obligations and statutory guidance.

A full breakdown of the information we collect on the school workforce can be found in the record of data processing which can be requested from Richard Lane, Director of Finance & Operations (email rlane@twyfordacademies.org.uk , phone 020 3301 3189).

## 2 Why we collect and use this information

The purpose of collecting and processing includes but is not limited to:

- Running the school in an effective and efficient manner
- Enabling you to be paid and other benefits to be provided
- Facilitating safeguarding as part of our safeguarding obligations towards pupils
- Fulfilling our legal obligations in recruiting individuals to the school workforce
- Supporting effective performance management and appraisal
- Supporting effective management of the school workforce, along with the implementation of school policies and procedures
- Providing feedback to your training centre and awarding body
- Informing our recruitment and retention policies
- Allowing better financial modelling, administration and planning
- Providing references where requested
- Equalities monitoring and reporting
- Responding to any school workforce issues
- Improving the management of workforce data across the sector
- Supporting the work of the School Teachers' Review Body
- Assessing the quality of our services
- Complying with the law regarding data sharing.

## 3 The lawful basis for using this data

These are defined under data protection legislation and for personally identifiably information are:

- To fulfil a contract with you
- You have given consent for one or more specific purposes
- Processing is necessary to comply with the school's legal obligations

- Processing is necessary to protect your vital interests
- Processing is necessary for tasks in the public interest or exercise of authority vested in the controller (the provision of education)
- Processing is necessary for the school's legitimate interests or the legitimate interests of a third party.

When we process special category information, which is deemed to be more sensitive, the following lawful basis are used:

- You have given explicit consent
- Employment, social security and social protection
- It is necessary to fulfil the school's obligations or your obligations
- It is necessary to protect your vital interests
- Processing is carried out by a foundation or not-for-profit organisation (includes religious, political or philosophical organisations and trade unions)
- Reasons of public interest in the area of public health.

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent and explain how you can withdraw consent if you wish to do so.

## 4 Collecting this information

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

## 5 How we store your data

We collect, store and process data for each member of the school workforce. The information is contained in a virtual or physical file which is kept secure and only used for purposes directly relevant to your employment.

Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our retention policy, a copy of which can be requested from Richard Lane, Director of Finance & Operations (email rlane@twyfordacademies.org.uk , phone 020 3301 3189).

## 6 Transferring Data Internationally

We may send your information to other countries where:

- we or a company we work with store information on computer servers based overseas; or
- we communicate with you when you are overseas.

We conduct due diligence on the companies we share data with and note whether they process data in the UK, EEA (which means the European Union, Liechtenstein, Norway and Iceland) or outside of the EEA.

The UK and countries in the EEA are obliged to adhere to the requirements of the GDPR and have equivalent legislation which confer the same level of protection to your personal data.

For organisations who process data outside the UK and EEA we will assess the circumstances of how this occurs and ensure there is no undue risk.

Additionally, we will assess if there are adequate legal provisions in place to transfer data outside of the UK.

## 7 Who we share information with

In order for us to legally, effectively and efficiently function we are required to share data with appropriate third parties, including but not limited to:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and information about headteacher performance and staff dismissals
- The Department for Education- to meet our legal obligations to share certain information.
- Educators and examining bodies-such as ensuring we adhere to examining regulations to guarantee the validity of examinations
- Training centres and awarding bodies-in order to provide information and feedback on your performance.
- Your families and representatives- such as in the event of an emergency
- Financial organisations e.g. Pension Scheme, HMRC
- Ofsted-during the course of a school inspection
- Suppliers and service providers – to enable them to provide the service we have contracted them for such as HR, payroll, IT.
- Central and local government- such as workforce analysis
- Our auditors - to ensure compliance with our legal obligations
- Health authorities (NHS) and Occupational Health and employee support schemes to ensure the wellbeing of our staff body
- Health and social welfare organisations
- Professional advisers and consultants- for us to develop our services and best provide our public service
- Trade Unions and Professional Associations - to enable them to provide the service their members require
- Charities and voluntary organisations
- Police forces, courts, tribunals, Security organisations- to create a secure workplace for all staff

- Professional bodies
- Employment & recruitment agencies and future employers - to support reference requests.

## 8 Why we share your information

In order to successfully perform our key functions, we need to share personal data with organisations

For example, we are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

We are required to share information about our staff with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

## 9 Data collection requirements:

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance.

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data.

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:

https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https://www.gov.uk/contact-dfe

## 10 Data Protection Rights

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- NOT provide information where it compromises the privacy of others
- Give you a copy of the information in an intelligible form.

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

In most cases, we will respond to subject access requests within 1 month, as required under data protection legislation However, we are able to extend this period by up to 2 months for complex requests or exceptional circumstances.

Your Other Rights regarding your Data:
You may:

- Withdraw your consent to processing at any time (This only relates to data for which the school relies on consent as a lawful basis for processing)
- Ask us to rectify, erase or restrict processing of your personal data, or object to the processing of it in certain circumstances and where sufficient supporting evidence is supplied
- Prevent the use of your personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest, official authority or legitimate interests.
- Request a copy of agreements under which your personal data is transferred outside of the United Kingdom.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect you)
- Request a cease to any processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Refer a complaint to the ICO

- Ask for your personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

If you would like to exercise any of the rights or requests listed above, please contact Richard Lane, Director of Finance & Operations (email: rlane@twyfordacademies.org.uk, phone: 020 3301 3189, address: Twyford C of E Academies Trust, Twyford Crescent, London W3 9PP).

The School will comply with the Data Protection legislation in regard to dealing with all data requests submitted in any format, although individuals are asked to preferably submit their request in written format to assist with comprehension.

We reserve the right to verify the requesters identification by asking for Photo ID. If this proves insufficient then further ID may be required.

## 11 Data Protection Breaches

If you suspect that your or someone else's data has been subject to unauthorised or unlawful processing, accidental loss, destruction or damage, we ask that you Richard Lane, Director of Finance & Operations (email: rlane@twyfordacademies.org.uk, phone: 020 3301 3189) and advise us without undue delay.

## 12 Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our independent data protection officer Claire Mehegan at the London Diocesan Board for Schools (claire.mehegan@london.anglican.org).

Alternatively, you can refer a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

## 13 Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact either our School Data Protection Lead, Richard Lane, Director of Finance & Operations (email: rlane@twyfordacademies.org.uk, phone: 020 3301 3189) or our independent Data Protection Officer, Claire Mehegan at the London Diocesan Board for Schools (claire.mehegan@london.anglican.org).

## Appendix C: Privacy Notice – Job Applicants

### How we use Job Applicants' Information

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals applying for jobs at our school.

Twyford Church of England Academies Trust is the 'Data controller' for the purposes of data protection law.

We have appointed Grow Education Partners Ltd as our data protection officer (DPO) and the responsible contact is Claire Mehegan (see 'Contact us' below).

Successful candidates will also need to refer to our privacy notice for the school workforce for information about how their personal data is collected, stored and used once they join the school.

### 1 The personal data we collect and hold

We process data relating to those applying to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not limited to:

- Personal information (such as name, date of birth, national insurance number)
- Contact details and preferences (such as telephone number, email address, postal address)
- Copies of right to work documentation
- References
- Evidence of qualifications
- Employment records (such as including work history, job titles, training records and professional memberships)
- Information about your criminal record
- Closed- circuit television (CCTV) Images
- Protected characteristics (such as race, ethnicity, religious beliefs, sexual orientation)
- Relevant Medical Information (such as disability and access requirements).

We may also hold personal data about you from third parties, such as references supplied by former employers or service users, information provided during the completion of our pre-employment checks, and from the Disclosure & Barring Service, in order to comply with our legal obligations and statutory guidance.

A full breakdown of the information we collect on Job applicants can be found in the record of data processing which can be requested from Richard Lane, Director of Finance & Operations (email rlane@twyfordacademies.org.uk , phone 020 3301 3189).

### 2 Why we collect and use this data

The purpose of collecting and processing this data includes but is not limited to:

- Staff recruitment and ensuring we have all the necessary information to enter into a contract with you
- Fulfilling our legal obligations, for example to check a successful applicant's eligibility to work in the UK before employment starts
- Enabling us to establish relevant experience and qualifications
- Facilitating safer recruitment, as part of our safeguarding obligations towards pupils
- Enabling equalities monitoring
- Ensuring that appropriate access arrangements can be provided for candidates that require them.

## 3 Our lawful basis for using this data

This section contains information about the legal basis that we are relying on when handling your information. These are defined under data protection legislation and for personally identifiable information are:

- You have given consent for one or more specific purposes
- Processing is necessary to fulfil a contract or to take specific steps before entering into a contract
- Processing is necessary to comply with the school's legal obligations
- Processing is necessary to protect your vital interests
- Processing is necessary for tasks in the public interest or exercise of authority vested in the controller (the provision of education).

When we process special category information, which is deemed to be more sensitive, the following lawful basis are used:

- You have given explicit consent
- It is necessary to fulfil the school's obligations or your obligations
- It is necessary to protect your vital interests
- Processing is carried out by a foundation or not-for-profit organisation (includes religious, political or philosophical organisations and trade unions)
- Reasons of public interest in the area of public health.

Where we have obtained consent to use personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn.

## 4 Collecting this information

While the majority of information we collect about you is mandatory, some information can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

## 5 How we store this data

Personal data we collect as part of the job application process is stored in line with our data protection policy. When it is no longer required, we will delete your information in accordance with our data retention policy. The Retention Policy can be requested from

Richard Lane, Director of Finance & Operations (email rlane@twyfordacademies.org.uk , phone 020 3301 3189).

## 6 Unsuccessful Candidates

If your application for employment is unsuccessful, the organisation will hold your data on file for 6 months after the end of the relevant recruitment process.

At the end of that period, your data is deleted or destroyed.

## 7 Who we share data with

In order for us to legally, effectively and efficiently function we are required to share data with appropriate third parties, including but not limited to

- Former employers – to obtain references
- Employment background check providers- to obtain necessary background checks
- Our auditors- to ensure our compliance with our legal obligations
- Our local authority – to meet our legal obligations to share certain information with it, such as shortlists of candidates for a headteacher position
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as HR and recruitment support
- Professional advisers and consultants
- Employment and recruitment agencies.

## 8 Transferring data internationally

We may send your information to other countries where:

- we or a company we work with store information on computer servers based overseas; or
- we communicate with you when you are overseas.

We conduct due diligence on the companies we share data with and note whether they process data in the UK, EEA (which means the European Union, Liechtenstein, Norway and Iceland) or outside of the EEA.

The UK and countries in the EEA are obliged to adhere to the requirements of the GDPR and have equivalent legislation which confer the same level of protection to your personal data.

From organisations who process data outside the UK and EEA we will assess the circumstances of how this occurs and ensure there is no undue risk.

Additionally, we will assess if there are adequate legal provisions in place to transfer data outside of the UK.

## 9 Data Protection Rights

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for

- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- NOT provide information where it compromises the privacy of others
- Give you a copy of the information in an intelligible form.

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

In most cases, we will respond to subject access requests within 1 month, as required under data protection legislation However, we are able to extend this period by up to 2 months for complex requests or exceptional circumstances.

Your Other Rights regarding your Data:

- Withdraw your consent to processing at any time (This only relates to data for which the school relies on consent as a lawful basis for processing)
- Ask us to rectify, erase or restrict processing of your personal data, or object to the processing of it in certain circumstances and where sufficient supporting evidence is supplied
- Prevent the use of your personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest, official authority or legitimate interests.
- Request a copy of agreements under which your personal data is transferred outside of the United Kingdom.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect you)
- Request a cease to any processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Submit a complaint to the ICO
- Ask for your personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

If you would like to exercise any of the rights or requests listed above, please contact Richard Lane, Director of Finance & Operations (email: rlane@twyfordacademies.org.uk, phone: 020 3301 3189, address: Twyford C of E Academies Trust, Twyford Crescent, London W3 9PP).

The School will comply with the data protection legislation in regard to dealing with all data requests submitted in any format, individuals are asked to preferably submit their request in written format to assist with comprehension.

We reserve the to verify the requesters identification by asking for Photo ID. If this proves insufficient then further ID may be required.

## 10 Data Protection Breaches

If you suspect that your or someone else's data has been subject to unauthorised or unlawful processing, accidental loss, destruction or damage, we ask that you Richard Lane, Director of Finance & Operations (email: rlane@twyfordacademies.org.uk, phone: 020 3301 3189) and advise us without undue delay.

## 11 Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our independent data protection officer Claire Mehegan at the London Diocesan Board for Schools (claire.mehegan@london.anglican.org).

Alternatively, you can refer a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

## 12 Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact either our School Data Protection Lead, Richard Lane, Director of Finance & Operations (email: rlane@twyfordacademies.org.uk, phone: 020 3301 3189) or our independent Data Protection Officer, Claire Mehegan at the London Diocesan Board for Schools (claire.mehegan@london.anglican.org).

## Appendix D: Privacy Notice – Members, Directors, Governors and other volunteers

How we use Members, Directors, Governors' and other Volunteers' Information

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals working with the school in a voluntary capacity, including Governors.

Twyford Church of England Academies Trust, ("the Trust"/"the School") is the 'Data controller' for the purposes of data protection law.

We have appointed Grow Education Partners Ltd as our data protection officer (DPO) and the responsible contact is Claire Mehegan (see 'Contact us' below).

### 1 The Personal Data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not limited to:

- Personal Information (such as name, date of birth, next of kin, dependents, marital status)
- Contact details (such as telephone number, email address, postal address, for you and your emergency contacts)
- Protected characteristics (such as trade union membership, nationality, language, ethnic origin, sexual orientation, health and religion or belief, where this has been provided)
- Relevant medical information (such as physical or mental health conditions, including for any disabilities which the organisation needs to make any reasonable adjustments to fulfil its duty of care)
- Qualifications, and employment records (such as work history, job titles, references, training records and professional memberships)
- Outcomes of any disciplinary and/or grievance procedures, including any warning issues to you and related correspondence
- Governor performance information (Such as meeting attendance, visits, roles, and leadership responsibilities)
- Information about business and pecuniary interests
- Information about your criminal record
- Closed-circuit television (CCTV) footage
- Data about your use of the school's information and communications system
- Photographs (for internal safeguarding & security purposes, school newsletters, media, and promotional purposes)
- Payment and banking details where required (e.g. for expense claims).

We may also hold personal data about you from third parties, such as information supplied by the appointing body and from the Disclosure & Barring Service, in order to comply with our legal obligations and statutory guidance.

A full breakdown of the information we collect on volunteers can be found in the record of data processing which can be requested from Richard Lane, Director of Finance & Operations (email rlane@twyfordacademies.org.uk , phone 020 3301 3189).

## 2 Why we collect and use this information

The reasons we collect and process this data includes but is not limited to:

- Establish and maintain effective governance
- Meet statutory obligations for publishing and sharing voluntary individuals' details
- Facilitate safeguarding as part of our safeguarding obligations towards pupils
- Fulfil our legal obligations in appointing voluntary individuals
- Support development
- Equalities monitoring and reporting
- Ensure that appropriate access arrangements can be provided for volunteers who require them
- To comply with the law regarding data sharing
- Respond to any school workforce issues
- Undertake statutory reporting the Department for Education.

## 3 The lawful basis on which we use this information

Are defined under data protection legislation and for personally identifiably information are:

- Processing is necessary to fulfil a contract with you
- You have given consent for one or more specific purposes
- Processing is necessary to comply with the school's legal obligations
- Processing is necessary to protect your vital interests
- Processing is necessary for tasks in the public interest or exercise of authority vested in the controller (the provision of education).
- Processing is necessary for the school's legitimate interests or the legitimate interests of a third party.

When we process special category information, which is deemed to be more sensitive, the following lawful basis are used:

- You have given explicit consent
- Employment, social security, and social protection
- It is necessary to fulfil the school's obligations or your obligations
- It is necessary to protect your vital interests
- Processing is carried out by a foundation or not-for-profit organisation (includes religious, political, or philosophical organisations and trade unions)
- Reasons of public interest around public health.

Where we have obtained consent to use personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn.

## 4 Collecting this information

While the majority of the information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

## 5 Storing your data

Personal data is stored in accordance with our data retention policy.

We retain personal information about all volunteers. This information is kept secure and is only used for purposes directly relevant to your work with the school.

When your relationship with the school has ended, we will retain and dispose of your personal information in accordance with our Data Retention Schedule. A copy of this can be obtained by contacting Richard Lane, Director of Finance & Operations (email rlane@twyfordacademies.org.uk , phone 020 3301 3189).

## 6 Who we share information with

In order for us to legally, effectively and efficiently function we are required to share data with appropriate third parties, including but not limited to:

- The Department for Education- to meet our legal obligations to share certain information.
- Our local authority – to meet our legal obligations to share certain information with it, such as details of governors
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as governor support and IT services
- Training centres and awarding bodies-in order to share information and feedback on your performance.
- Your families and representatives- such as in the event of an emergency
- Our auditors to ensure compliance with our legal obligations
- Trade Unions and Professional Associations - to enable them to provide the service their members require
- Professional advisers and consultants - for us to develop our services and best provide our public service
- Employment & recruitment agencies and future employers - to support reference requests
- Police forces, courts, tribunals, security organisations- to create a secure workplace for all at the school.
- Charities and voluntary organisations.

## 7 Transferring data internationally

We may send your information to other countries where:

- we or a company we work with store information on computer servers based overseas; or
- we communicate with you when you are overseas.

We conduct due diligence on the companies we share data with and note whether they process data in the UK, EEA (which means the European Union, Liechtenstein, Norway and Iceland) or outside of the EEA.

The UK and countries in the EEA are obliged to adhere to the requirements of the GDPR and have equivalent legislation which confer the same level of protection to your personal data.

For organisations who process data outside the UK and EEA we will assess the circumstances of how this occurs and ensure there is no undue risk.

Additionally, we will assess if there are adequate legal provisions in place to transfer data outside of the UK.

## 8 Why we share your information

In order to successfully perform our key functions, we need to share personal data with organisations for example we share personal data with the Department for Education (DfE) on a statutory basis. Under s.538 of the Education Act 1996, and the Academies Financial Handbook, the Secretary of State requires boards to provide certain details they hold about people involved in governance, as volunteered by individuals, and the information kept up to date.

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

For more information about the department's data sharing process, please visit:

https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https://www.gov.uk/contact-dfe

## 9 Data Protection Rights

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- NOT provide information where it compromises the privacy of others
- Give you a copy of the information in an intelligible form.

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

In most cases, we will respond to subject access requests within 1 month, as required under data protection legislation However, we are able to extend this period by up to 2 months for complex requests or exceptional circumstances.

### Your Other Rights regarding your Data

You may:

- Withdraw your consent to processing at any time (This only relates to data for which the school relies on consent as a lawful basis for processing)
- Ask us to rectify, erase or restrict processing of your personal data, or object to the processing of it in certain circumstances and where sufficient supporting evidence is supplied
- Prevent the use of your personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest, official authority or legitimate interests.
- Request a copy of agreements under which your personal data is transferred outside of the United Kingdom.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect you)
- Request a cease to any processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Submit a complaint to the ICO
- Ask for your personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

If you would like to exercise any of the rights or requests listed above, please contact Richard Lane, Director of Finance & Operations (email: rlane@twyfordacademies.org.uk, phone: 020 3301 3189, address: Twyford C of E Academies Trust, Twyford Crescent, London W3 9PP).

The School will comply with the Data Protection legislation in regard to dealing with all data requests submitted in any format, although individuals are asked to preferably submit their request in written format to assist with comprehension.

We reserve the right to verify the requesters identification by asking for Photo ID. If this proves insufficient then further ID may be required.

## 10 Data Protection Breaches

If you suspect that your or someone else's data has been subject to unauthorised or unlawful processing, accidental loss, destruction or damage, we ask that you please Richard Lane, Director of Finance & Operations (email: rlane@twyfordacademies.org.uk, phone: 020 3301 3189) and advise us without undue delay.

## 11 Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our independent data protection officer Claire Mehegan at the London Diocesan Board for Schools (claire.mehegan@london.anglican.org).

Alternatively, you can refer a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

## 12 Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact either our School Data Protection Lead, Richard Lane, Director of Finance & Operations (email: rlane@twyfordacademies.org.uk, phone: 020 3301 3189) or our independent Data Protection Officer, Claire Mehegan at the London Diocesan Board for Schools (claire.mehegan@london.anglican.org).

**Appendix E: Guidelines Concerning Different Circumstances in which Sensitive Personal Information May be Disclosed.**

**1. In the classroom**

In the classroom in the course of a lesson given by a member of teaching staff or an outside visitor, including health professionals.

Careful thought needs to be given to the content of the lesson, setting the climate and establishing ground rules to ensure confidential disclosures are not made. It should be made clear to pupils that this is not the time or place to disclose confidential, personal information.

When a health professional is contributing to a school health education programme in a classroom setting, s/he is working with the same boundaries of confidentiality as a teacher.

**2. One to one disclosures to members of school staff (including voluntary staff).**

It is essential that all members of staff know the limits of the confidentiality they can offer to both pupils and parents/carers (see note below) and any required actions and sources of further support or help available both for the pupil or parent/carer and for the staff member within the school and from other agencies, where appropriate. All staff at this school encourage pupils to discuss difficult issues with their parents or carers, and vice versa. However, the needs of the pupil are paramount and school staff will not automatically share information about the pupil with his/her parents/carers unless it is considered to be in the child's best interests.

(Note: That is, that when concerns for a child or young person come to the attention of staff, for example through observation of behaviour or injuries or disclosure, however insignificant this might appear to be, the member of staff should discuss this with a member of the Child Protection team as soon as is practically possible. More serious concerns must be reported immediately to ensure that any intervention necessary to protect the child is accessed as early as possible. Please see the school Child Protection Policy.)

Although teachers are not legally bound to inform parents/carers or the head teacher following a disclosure of pregnancy by a pupil, it is school policy that such information should be reported to the Child Protection Team. Teachers should seek consent for such a disclosure and should make clear they cannot offer or guarantee pupils unconditional confidentiality.

**3. Disclosures to a counsellor, school nurse or health professional operating a confidential service in the school.**

Health professionals such as school nurses can give confidential medical advice to pupils provided they are competent to do so and follow the Fraser Guidelines (guidelines for doctors and other health professionals on giving medical advice to under 16s). School nurses are skilled in discussing issues and possible actions with young people and always have in mind the need to encourage pupils to discuss issues with their parents or carers. However, the needs of the pupil are paramount

and the school nurse will not insist that a pupil's parents or carers are informed about any advice or treatment they give.

***The principles we follow are that in all cases we:***

- Ensure the time and place are appropriate, when they are not we reassure the child that we understand they need to discuss something very important and that it warrants time, space and privacy.
- See the child normally (and always in cases of neglect, or abuse) before the end of the school day. More serious concerns must be reported immediately to ensure that any intervention necessary to protect the child is accessed as early as possible.
- Tell the child we cannot guarantee confidentiality if we think they will:
    - Hurt themselves
    - Hurt someone else
    - Or they tell us that someone is hurting them or others
- Not interrogate the child or ask leading questions
- Not put pupils in the position of having to repeat distressing matters to several people
- Inform the pupil first before any confidential information is shared, with the reasons for this
- Encourage the pupil, whenever possible to confide in his/her own parents/carers

At Trust schools, teaching staff should discuss any concerns about pupils with the Child protection team. Teaching assistants and mentors should discuss with the SENCo and/or the Child Protection team.

***Parents/carers:***

The Trust believes that it is essential to work in partnership with parents and carers and we endeavour to keep parents/carers abreast of their child's progress at school, including any concerns about their progress or behaviour. However, we also need to maintain a balance so that our pupils can share any concerns and ask for help when they need it. Where a pupil does discuss a difficult personal matter with staff at Trust schools, they will be encouraged to also discuss the matter with their parent or carer themselves.

The safety, well-being and protection of our pupils is the paramount consideration in all decisions staff at this school make about confidentiality.

***Onward referral:***

A member of the Child Protection team or the SENCO, is responsible for referring pupils to the school counsellor/mentor and to outside agencies from the school. Where there are areas of doubt about the sharing of information, advice will be sought from the local social services team. Staff should not make referrals themselves unless they believe a child protection referral to the police or SSD is

necessary and the designated person does not agree. ('What to do if you're worried a child is being abused', DfES, HO, etc., 2003).

***Students over the age of 18:***

The rights and responsibilities of students over the age of 18 – and their parents – differ from those of students under 18. Legal advice should be sought if issues arise which may need to be handled in a different way to reflect this.

**Appendix F: Sharing Sensitive Personal Information with other Agencies**

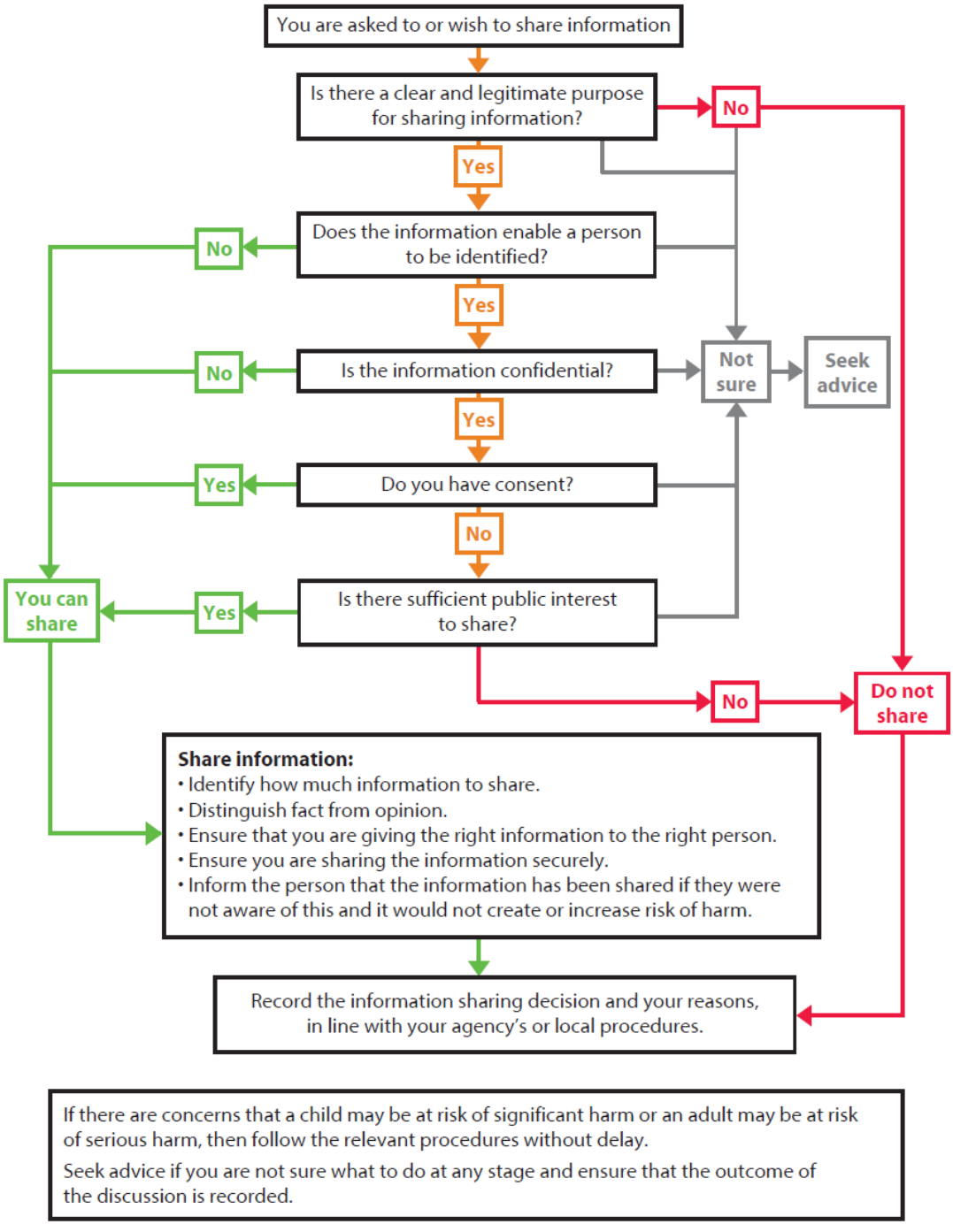
The school is guided by the Seven Golden Rules for information sharing as given by the DFE and the publication: *Information Sharing: Guidance for Practitioners and managers HM Government 2009.* The seven golden rules are:

1. Remember the Data Protection Act is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately
2. Be open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom the information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3. Seek advice if you are in any doubt, without disclosing the identity of the person where possible.
4. Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will have to base your judgement on the facts of the case.
5. Consider safety and well-being: Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.
6. Necessary, proportionate, relevant, accurate, timely and secure: Ensure the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.
7. Keep a record of your decision and the reason for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

The flowchart on the next page helps guide information sharing decisions.

HM Government

# Flowchart of key questions for information sharing



**Appendix G: Procedure for responding to subject access requests**

***Rights of access to information***

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

1. Under the Data Protection Act 2018 any individual has the right to make a request to access the personal information held about them.
2. The right of those (primarily parents) entitled to have access to curricular and educational records of individual pupils as defined within the Education Pupil Information (Wales) Regulations 2004.

These procedures relate to subject access requests made under the Data Protection Act 2018 and GDPR.

***Actioning a subject access request***

1. Requests for information may be verbal or in writing, including email. All requests received by staff must be passed on without delay to the Trust Data Team. If the initial request does not clearly identify the information required, then further enquiries will be made.
2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can 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.
3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 13 or above) and the nature of the request. The Executive Headteacher should 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. 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.
4. The school may not make a charge for the provision of information unless the requested is unfounded, excessive or a repeat request, in which case a fee related to the cost of providing the information may be charged.
5. The response time for subject access requests, once officially received, is 1 month.

6. The Data Protection Act 2018 allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure.
7. 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 should normally be obtained. There is still a need to adhere to the 1 month statutory timescale.
8. 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.
9. If there are concerns over the disclosure of information then additional advice should be sought.
10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.
11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.
12. Information can be provided at the 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 should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

## Appendix H: Model Information Sharing Agreement

In relation to ……:

Twyford C of E Academies Trust

and

…….

## 1. Introduction

### 1.1 Basis/Purpose for Sharing

A range of information will need to be shared between the two organisations to enable …….. The information to be shared may include personal information relating to staff and students.

### 1.2 Length of agreement

This agreement will commence at …….. and remain in place until terminated by either party.

### 1.3 Key Contacts

The key contacts in each organisation are:

Twyford C of E Academies Trust: Richard Lane, Director of Finance & Operations

…….. Trust: ??????????????.

## 2. Information Sharing

### 2.1 Type of information that may be shared

Personal information concerning staff and students: e.g. name, address, date of birth, next of kin, doctor etc.

Sensitive information concerning staff and students: e.g. ethnic origin, health, criminal offences, pay, performance, human resources file contents, student file contents.

### 2.2 How the information will be shared

Data may be shared via email provided files are appropriately secured/encrypted and passwords are notified by another, secure medium such as a phone call or text message.

Data will be shared on an ad hoc basis.

Information will be shared on a strict need to know basis only and the data will only be processed by staff in order for them to perform their duties in accordance with one or more of the defined purposes.

Under no circumstances should personal data be processed in any way that is unsecure or left unattended. It is the responsibility of the sender to ensure that the method is secure and that they have the correct contact details for the receiver.

**2.3 Recipients and other organisations that the information may be shared with.**

Information shared under this agreement may not be shared with third parties without further agreement.

**2.4 Data Quality**

Data will be checked/validated for accuracy before transmission.

**2.5 Retention and destruction**

Data will not be retained for longer than 10 years.

**2.6 Data subject rights**

Subject access requests should be addressed to the contacts referred to in paragraph 1.4. Shared information may be subject to a Freedom of Information Request. Personal information is exempt from disclosure under the Freedom of Information Act.

**2.7 Data Security**

Data may only be held in electronic form on systems complying with industry security standards.

## 3. Review and Termination of Agreement

This agreement will be reviewed by dd/mm/yyyy and may be terminated by either party giving 7 days' notice. Obligations concerning retention and security of data remain operative following the termination of this agreement.

## 4. Signatures

Signed for and on behalf of Twyford C of E Academies Trust of Twyford Crescent, Acton, London W3 9PP

Name: Richard Lane

| | |
|---|---|
| Position: | Director of Finance & Operations |
| Signature: | |
| Date: | dd/mm/yyyy |

| | | | |
|---|---|---|---|
| DPA Registration No. | Z3648440 | Date of expiry: | dd/mm/yyyy |

Signed for and on behalf of …….

| | |
|---|---|
| Name: | |
| Position: | |
| Signature: | |
| Date: | |

| | | | |
|---|---|---|---|
| DPA Registration No. | | Date of expiry: | |

**Appendix I: Privacy Impact Assessment**

Project Title: _____

1. Is a PIA required? Initial screening questions (More ticks indicates a full PIA is required):

| | ☑/☒ |
|---|---|
| • Will the project involve the collection of new information about individuals? | ☐ |
| • Will the project compel individuals to provide information about themselves? | ☐ |
| • Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? | |
| • Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? | ☐ |
| • Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition. | ☐ |
| • Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them? | ☐ |
| • Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private. | ☐ |
| • Will the project require you to contact individuals in ways which they may find intrusive? | ☐ |
| | ☐ |

2. Summarise the objective of the project and why a PIA is required:

3. Describe the information flows (The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.)

4. Identify the privacy and related risks

| Privacy Issue | Risk to individuals | Compliance risk | Associated risk to the Trust |
|---|---|---|---|
| | | | |

5. Identify the privacy solutions

| Risk | Solution/Mitigation | Result: Is the risk eliminated/reduced or accepted? | Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project? |
|---|---|---|---|
| | | | |

6. Sign off and record the PIA outcomes

| Risk | Approved solution/action | By who/by when | Approved by |
|---|---|---|---|
| | | | |