



Twyford
C of E
Academies Trust

Document Title	Data Protection and Confidentiality Policy
Committee Responsible for Policy	Resources
Review Frequency	Every 3 years
Last Reviewed	November 2017
Next Review Due	November 2020
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: 11/3/2015
1. What is the potential for this policy impacting a person or group with a protected characteristic differently (favourably or unfavourably) from everyone else?	
The policy may have greater application to people in protected groups as sensitive information about their protected characteristics (eg 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?	
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?	
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?	
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?	
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 the Data Protection Act 1998, the General Data Protection Regulation (EU 2016/679) (GDPR), and other related legislation. 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.

1 Policy Statement

The Trust is fully committed to compliance with the requirements of the Data Protection Act 1998, the General Data Protection Regulation (EU 2016/679) (GDPR), the Children’s Act 2004 and other relevant Acts of parliament or regulations insofar as they create duties on Controllers and Processors (the Twyford Trust is both) concerning the use of personal information. 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

The Data Protection Act and GDPR make 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.

Under the GDPR, it 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 or condition;
- 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 (*GDPR Article 5*). 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 the GDPR 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

The GDPR requires that Controllers are explicit about the legal basis for processing personal information. In the case of the Trust, for most processing the legal basis is *GDPR Article 6(1)(e)* – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. However, where personal data is processed for reasons not covered by this justification, consent of the data subjects is required (by means of either a paper or online consent form). For pupils under 16, the consent of a parent is required.

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 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 statement which explains who will use the information and for what purpose (see appendices A and B) 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 C.

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 showing personal information should never be left out 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 held in a secure location for no longer than 1 year.
- 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.

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 and B).
- 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.
- 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.
- 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.
- 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 D. 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 F. 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.

2.6 Subject Access Requests

If the Trust receives a written request from a data subject to see any or all personal data that the Trust holds about them this will be treated as a legitimate Subject Access Request and 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.

Informal requests to view or have copies of personal data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the Trust will comply within the 1 month time limit.

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

3 Responsibilities and Accountability

The GDPR has created additional obligations on 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 G.

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 the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other 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 DPO 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 DPO.

Appendix A: Privacy Notice – Pupils/Parents

Who are we?

The Twyford C of E Academies Trust, Twyford Crescent, London W3 9PP is the Data Controller for the purposes of the Data Protection Act 1998 and the General Data Protection Regulation (EU 2016/679) (GDPR).

Why do we collect and use pupil information?

We collect and use personal information to perform a task carried out in the public interest and in the exercise of official authority (*GDPR Article 6 1(e)*) and sensitive personal information also for reasons of substantial public interest on the basis of law (*GDPR Article 9 2(g)*). The specific legal basis for the collection of pupil information is the Education Act 1996. We collect information from you and may receive information about you from your previous school and the Learning Records Service. We hold this pupil data and use it to:

- Support pupil learning;
- Monitor and report on pupil progress;
- Provide appropriate pastoral care;
- Assess the quality of our services;
- Comply with the law regarding data sharing.

What information is collected?

- Personal information (such as name, unique pupil number, address, details of parents and other contacts);
- Characteristics (such as ethnicity, language, nationality, country of birth, and free school meal eligibility);
- Assessment information;
- Attendance information (such as sessions attended, number of absences and absence reasons);
- Exclusions and behavioural information;
- Special educational needs and medical information;
- Post 16 learning information including bursary eligibility and progression information.

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the GDPR, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

We hold pupil data for up to 25 years so that we are able to respond to requests from former pupils for details of their education including qualifications.

Who do we share pupil information with?

We routinely share pupil information with:

- schools that the pupil's attend after leaving us;
- our/your local authority;
- the Department for Education (DfE);
- The National Health Service.

Aged 14+ qualifications

For pupils enrolling for post 14 qualifications, the Learning Records Service will give us a pupil's unique learner number (ULN) and may also give us details about the pupil's learning or qualifications

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so. We do not expect to transfer data to a non-EU country for offsite storage or processing but if we did we would ensure that appropriate safeguards were in place.

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 the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

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>.

Youth support services

What is different about pupils aged 13+?

Once our pupils reach the age of 13, we also pass pupil information 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

A parent / guardian can request that only their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / pupil once he/she reaches the age 16.

Our pupils aged 16+

We will also share certain 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.

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>

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the Trust Data Team (datateam@twyfordacademies.org.uk).

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at <https://ico.org.uk/concerns/>

Contact:

If you would like to discuss anything in this privacy notice, please contact, Richard Lane (rlane@twyford.ealing.sch.uk 020 8752 0141) or the Trust's Data Protection Officer, Robert Bullett at the London Diocesan Board for Schools, London Diocesan House, 36 Causton Street, London SW1P 4AU (robert.bullett@london.anglican.org 020 7932 1161).

Appendix B: Privacy Notice - Staff

Who are we?

The Twyford C of E Academies Trust, Twyford Crescent, London W3 9PP is the Data Controller for the purposes of the Data Protection Act 1998 and the General Data Protection Regulation (EU 2016/679) (GDPR).

Why do we collect and use staff information?

We collect and use personal information to perform a task carried out in the public interest and in the exercise of official authority (*GDPR Article 6 1(e)*) and sensitive personal information also for reasons of substantial public interest on the basis of law (*GDPR Article 9 2(g)*). The specific legal basis for the collection of school staff information is the Education Act 1996. We collect information from you and may receive information about you from your previous school and the Disclosure and Barring Service. We hold this data and use it to:

- improving the management of workforce data across the sector
- enabling development of a comprehensive picture of the workforce and how it is deployed
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling ethnicity and disability monitoring; and
- supporting the work of the School Teachers' Review Body

What information is collected?

- Personal information (such as name, National Insurance number, address and next of kin);
- Characteristics (such as ethnicity, disabilities and nationality);
- Details of employment contracts, attendance, hours worked and remuneration details;

Collecting staff information

Whilst some of the information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the GDPR, we will inform you whether you are required to provide certain information to us or if you have a choice in this.

Storing pupil data

We may hold staff data for up to 25 years so that we are able to respond to requests from former staff for details of their pay and pension entitlements.

Who do we share staff information with and why do we share it?

We will not share information about you with third parties without your consent unless the law allows us to. We are required, by law, to pass on some of this personal data to:

- our local authority
- the Department for Education (DfE)

We do not expect to transfer data to a non-EU country for offsite storage or processing but if we did we would ensure that appropriate safeguards were in place.

DfE Data collection requirements

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 staff 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>

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

Requesting access to your personal data

Under data protection legislation, staff have the right to request access to information about them that we hold. To make a request for your personal information contact the Trust HR Team (hr@twyford.ealing.sch.uk).

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at <https://ico.org.uk/concerns/>

Contact:

If you would like to discuss anything in this privacy notice, please contact, Richard Lane (rlane@twyford.ealing.sch.uk 020 8752 0141) or the Trust's Data Protection Officer, Robert Bullett at the London Diocesan Board for Schools, London Diocesan House, 36 Causton Street, London SW1P 4AU (robert.bullett@london.anglican.org 020 7932 1161).

Appendix C: 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.

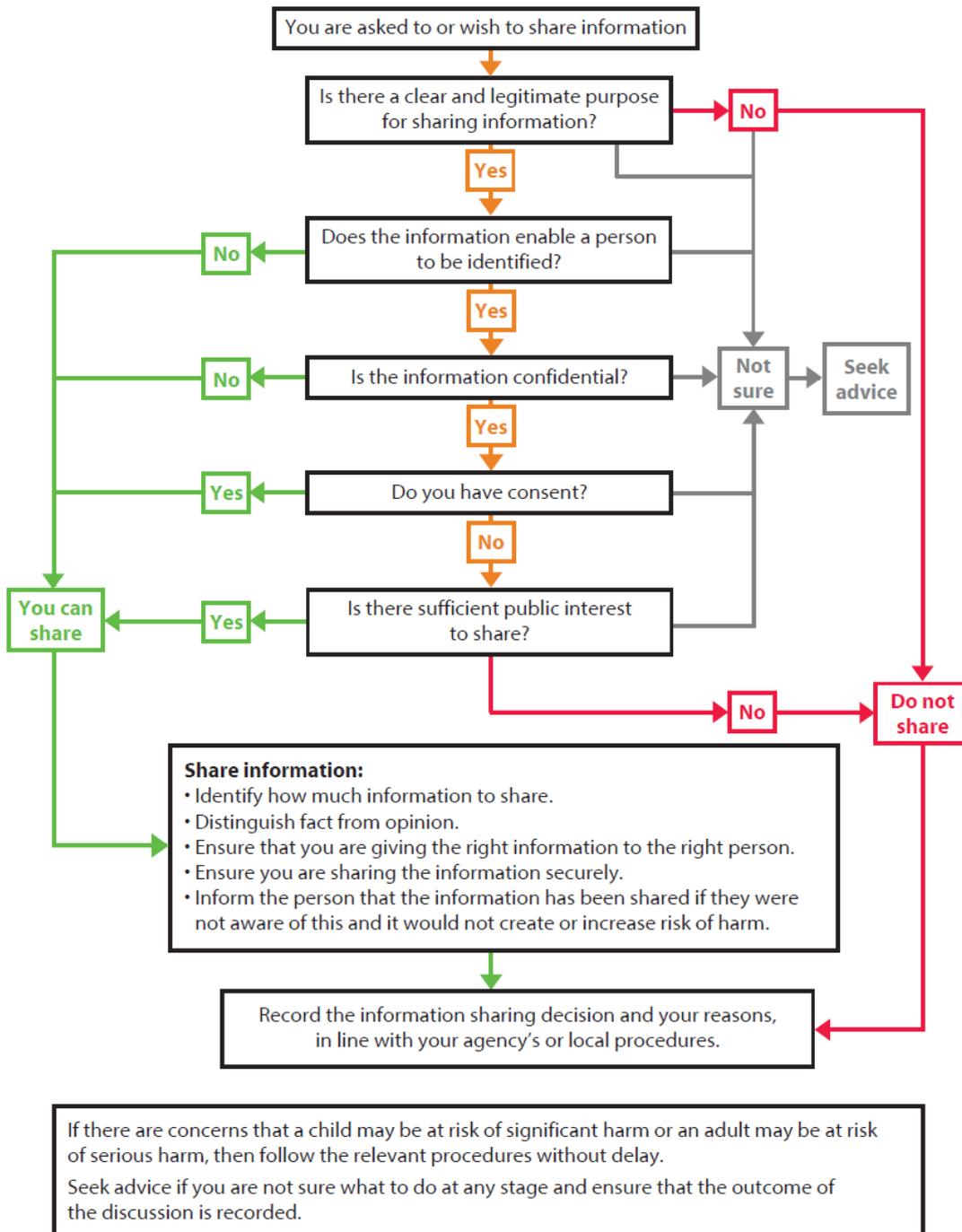
Appendix D: Sharing Sensitive Personal Information with other Agencies

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.

Flowchart of key questions for information sharing



Appendix E: 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 1998 any individual has the right to make a request to access the personal information held about them. This right is reinforced and tightened up in the GDPR.
2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

These procedures relate to subject access requests made under the Data Protection Act 1998 and GDPR.

Actioning a subject access request

1. Requests for information must be made in writing; which includes email, and be addressed to the Trust Data Team in the first instance. 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 12 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 1998 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 F: 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: eg name, address, date of birth, next of kin, doctor etc

Sensitive information concerning staff and students: eg 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

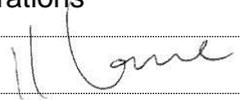
Data may only be held in electronic form on systems complying with industry security standards.

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 G: 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?	<input type="checkbox"/>
• Will the project compel individuals to provide information about themselves?	<input type="checkbox"/>
• Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	<input type="checkbox"/>
• Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	<input type="checkbox"/>
• 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.	<input type="checkbox"/>
• Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	<input type="checkbox"/>
• 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.	<input type="checkbox"/>
• Will the project require you to contact individuals in ways which they may find intrusive?	<input type="checkbox"/>

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