Twynham Learning

Data Protection Policy

Reviewed by Vicky Elsworth, HR Manager and Anusha Hesketh, Governance Manager November 2020

Ratified by the Board of Trustees 16.12.20

Next review date May 2021

This policy has been reviewed in line with the 8 principles set out in the Single Equality Policy and an initial screening Equality Impact Assessment has been carried out.

Within this policy the term Headteacher refers to the Headteacher of the school and the term CEO refers to the Chief Executive Officer of the Twynham Learning Academy Trust (the Trust).

The Governors of the Trust are charity trustees and company directors and for the purpose of this policy these terms are interchangeable.

This policy reflects the legislation at the time that it was last reviewed. Any changes in legislation will take precedence over anything printed in this policy.

Context and overview

Each school within our Trust needs to gather and use certain personal information about individuals. This can include learners, parents, staff and Governors.

All data must be collected, stored and managed in accordance with UK and EU law, and in line with our school ethos and values. Individuals retain the rights over their own data at all times. Our use of their data must be fair and lawful, and we must be open and honest about what we do with people's data.

All data we process is in accordance with the rules as laid down in statute, including the General Data Protection Regulations (and the Data Protection Act 2018), the Education Act 1986, the Education and Skills Act 2008, Protection of Freedoms Act 2012 and the Apprenticeship, Skills, Children and Learning Act 2009 and the DfE (2018) ‘Protection of biometric information of children in schools and colleges’.

Key principles

- Individuals retain rights over their data
- Data should be collected fairly and lawfully and used only in ways that the individual would expect
- Data should only be kept for as long as is necessary
- Data integrity and security is paramount
- Data governance will be actively managed at all levels of the organisation, to minimise risks to both the individual and the organisation
- All collection and use of data will be open and honest

Why this policy exists

This policy will help ensure that each school within our Trust respects the rights of all individuals whose data it collects, including learners, parents, staff and Governors. It encompasses legal responsibilities and best practice. By being open and honest with individuals we will demonstrate that people can trust our organisation and that we handle personal data with integrity. Routine application of these principles will also help protect our schools from the risk of data breaches and unauthorised access to personal information.

Data Protection Law and Principles

The use of personal data is governed by EU and UK law. In order to comply with the law, personal data must be collected fairly and lawfully. It must be stored safely and managed securely. It must not be disclosed to anyone who does not have authority to see it.

The General Data Protection Regulations (GDPR) set out how data should be obtained, stored and handled. These regulations set out six principles that underpin lawful use of data. These provide the foundation for good data governance. These principles are enhanced by a range of powers for individuals to control how data their processed and stored.

Policy Scope

This policy applies to:

- All schools within our organisation.
- All teaching staff and support staff.
- Trustees, Governors and volunteers.
- Contractors, suppliers and anyone working on our behalf

Responsibilities under this policy

Everyone who works with or for Twynham Learning, or for or with one of our schools, has some responsibility for ensuring that data is handled safely, securely and appropriately.

There are key roles within the organisation that carry specific responsibilities.

The Board of Trustees is the strategic lead body for the Trust. They will bear ultimate responsibility for ensuring that all our legal obligations are met. They will be accountable for any failure to abide by the correct regulations and for any impact that they may have on our learning community and our reputation within the local area.

The Headteacher and Senior Leadership Team are the operational lead body within each school. They must ensure that all relevant policies and procedures are in place, and that practice follows the policy across all teams and school areas. They will liaise with the Data Protection Officer in the event of any data governance issues that require attention, and will have overall responsibility for setting an appropriate tome of respect for personal data within the school.

The Data Protection Officer has a key role to play in providing expert advice and guidance to the Board and the Senior Leadership Team. It is their responsibility to update senior management and the Board about Data Protection issues, and update policies and procedures in accordance with an agreed schedule and following legislative and best practice updates. They will oversee training and guidance for all staff, and be responsible for liaison with 3rd party suppliers, contractors and partners if they handle personal data. They will liaise with any 3rd party used for processing data, such as an HR / payroll supplier or cloud computing provider, to ensure appropriate levels of protection for all personal data. They will also oversee any Subject Access Requests, and handle the response to any data breaches, including being the point of contact for the public and notifying the ICO where necessary.

Each school has appointed a lead person for Data Protection who will take a lead on day to day matters regarding Data Protection.

The Communications Officer has responsibility for making sure that customer-facing applications such as websites or online forms owned or operated by our Trust comply with relevant regulations. They are also responsible for overseeing the timely distribution of Privacy Notices.

The Executive Data Manager has responsibility for advising across the Trust in regards to the Data Retention Policy, best practice in keeping data up to date and accurate, and best practice in the use of the MIS to store the vast majority of pupil and staff data.

The Executive IT Manager is responsible for ensuring the physical and virtual integrity of IT data storage services, systems and equipment. They will ensure all IT security meets acceptable professional standards, appropriate to the needs of the organisation, and that access to all electronic systems, databases or files is managed in accordance with the relevant polices. They will also oversee the life-cycle of software and hardware, and ensure that the process for encrypting files functions effectively.

The Executive Clerk and the Clerks to the Governors across the Trust will be responsible for the secure storage of personal data relating to the Governors and Trustees. They will keep this data up to date and store it in line with the retention guidelines.

What is personal data?

Personal data is information about a person - anything that would allow someone to identify a living individual, including biometric data (e.g. fingerprints). Processing that data means obtaining, using, and transferring data, and storing it in any system that allows it to be found again, such as a computer database or filing system.

Special category data

Special category data has been defined as data that poses more significant risk should it be shared. The data is more sensitive and, therefore, needs more protection when being collated and processed. Special category data includes:

- Race
- Ethnic origin
- Political interest
- Religion
- Trade union membership
- Genetics
- Biometric data used for ID purposes
- Health
- Sexual orientation

Our Privacy Notices

Each school within the Trust will take all reasonable steps to ensure that individuals are aware of how their data is being processed. This will include telling individuals what is being used, how it is being used, how long it will be kept for, and how they can exercise their rights in respect of that data.

Each school has a Privacy Notice for students' data, setting out how we collect data, what data we collect, the lawful basis for having the data, and how long we retain it. It includes information on who we share data with and the lawful basis for such sharing. It also sets out how people can request copies of data we hold about them. The Notice will be included in admissions documentation. A copy of the Privacy Notice for Twynham School is included at Appendix 1. This has been adapted by the other schools in the Trust to suit their needs.

Twynham Learning has put together a Privacy Notice for staff data, setting out how we collect data, what data we collect, the lawful basis for that, and how long we retain it. It includes information on who we share data with and the lawful basis for such sharing. It also sets out how people can request copies of data we hold about them. It will be included in the Staff Induction Pack across the schools. The Privacy Notice for Twynham School is included at Appendix 2. It has been adapted very slightly for the other schools in the Trust.

The privacy notices will be updated when the schools or the Trust decide to share data with new organisations.

Keeping personal data secure

Once personal data has been lawfully and fairly collected and processed, it must be safely stored, kept up to date, and safely accessed. Storing data in a way that complies with the regulations is a mix of common sense, clear processes and application of strong IT solutions.

The only people who will have access to personal data across our schools are those who need it for their work. Our IT systems and file storage have granular levels of permission, and we will ensure that people only see personal data if required for operational reasons or for the benefit of teaching and learning.

Strong passwords must be used to access electronic resources and IT systems. These should never be shared with other people, or written down. Guidance to staff as to how to choose a secure password is included at Appendix 3.

Personal data must only be disclosed to those who are authorised to see it, both within and outside the organisation. If there is any doubt about the identity of the person requesting access to information, or doubt as to whether they should be allowed to see it, the information should not be disclosed.

Data will only be shared with those people who are authorised to see it. This will be in line with our legal obligations and with the lawful and legitimate requirements of the business. Our Privacy Notices explains who we might share data with, the lawful basis for that, and the circumstances in which you can object to data being shared.

Full training for all staff will be available. This will help them understand their responsibilities under data protection legislation. Staff should ask their line manager or the Data Protection Officer for guidance if they are unsure about any aspect of data protection.

Data use, transfer and sharing

Data must only be used for the purpose it was first obtained. Personal data should not be shared informally, either internally or externally to the organisation.

Staff should follow simple checks when transferring data outside the schools via post or email, to ensure that personal data goes to the correct recipient. Staff across our sites will use a simple checklist, as per Appendix 4, when sending personal data by post in order to add an extra layer of security and checking.

Extra care must be taken when sharing data via email. This might include encryption or use of a secure email client. Password-protected documents must not be sent in the same email or to the same email address as the password itself; we recommend that a phone call is made to establish what the password is. All email recipients should be checked before the email is sent to ensure that it is not sent to the wrong person.

Data should not be stored on personal IT devices. In particular staff must not email school documents to their personal email addresses. If data needs to be transferred outside of the secure school environment, staff should use their school email account or a secure cloud storage solution such as Dropbox.

When receiving telephone calls requesting personal data for staff, students, parents or governors, there are procedures for staff to follow depending on who is calling and how easy it is to verify their identity. These are detailed in Appendix 5.

Projects involving the sharing or processing of a large amount of data, including processing biometric data should be assessed under a Data Protection Impact Assessment in the initial stages. This could be conducted by the Data Protection Officer or the member of staff with day to day responsibility for data protection at each site. A template is included at Appendix 6.

Data Retention and Disposal

Personal data in both electronic and paper form relating to our Primary School students will be passed in a timely and secure fashion to the destination school of the pupil. No record will then be held by the Primary School. Safeguarding records and the Accident Book are exempt from this retention period.

Personal data in both electronic and paper form relating to our Secondary School students will be retained securely on site until the student reaches the age of 25 years. This is to allow for references to be written and for us to be able to respond to enquiries from former students.

Staff records will be retained for 6 years following the termination of employment, to allow for any necessary proceedings to be completed and for references to be written.

Governor records will be retained for 2 years following the cessation of governance, to allow us to meet our reporting obligations.

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Marketing and Promotion

Marketing materials are produced at all sites, for example school prospectuses and newsletters. Where these feature images of students, we will have sought the relevant consent from either the parent or the student beforehand. Members of staff will be asked to provide their permission in writing.

In addition, Twynham Sixth Form asks students to enter personal details into their website when requesting a prospectus or booking an Open Morning. When doing this, we let all prospective parents and students know how their data will be stored, how often we might contact them, and give them the opportunity to decline to be contacted in the future.

Other schools follow a procedure of parents ringing the school directly to book a place on an Open Morning. In this case, they will be asked for their name and their child's name. This information will be securely disposed of once the Open Morning has passed.

We do not send out marketing materials from any of our sites. If Twynham Sixth Form send out a prospectus, this is on the back of a request from either the student or the parent and they have freely provided the information necessary to make this possible.

CCTV

Twynham School and The Grange School currently have internal CCTV in place in order to protect the assets provided for student and staff use in ICT teaching rooms. Images recorded by the internal CCTV cameras are stored on a separate server, in a secure location. They are retained for a maximum of 7 days, after which time they are securely overwritten.

Twynham School, Twynham Primary School, Stourfield Infant School and Stourfield Junior School all have external CCTV in place. This is to ensure the safety and security of those in our learning community, and to protect the site from damage. Our use of CCTV follows best practice guidelines as laid down by the ICO.

Images recorded by the CCTV cameras are stored on a separate server, in a secure location on each site. They are retained for a maximum of 7 days, after which time they are securely overwritten.

Access to the images is restricted to specified people within each school. We only view CCTV footage in response to an incident or an allegation.

The images on our CCTV system are of a sufficient quality to allow us to make out faces of individuals in most circumstances. We are able to take copies of relevant parts of the CCTV footage and store it securely, in order to assist investigations into incidents or allegations.

In certain circumstances we may share CCTV footage with partners or other agencies. This may include senior leaders, parents, the Local Authority or the Police.

Websites

Each school has its own website which carries a website-specific privacy policy addressing what happens when users fill in the forms available to them. Each school website also has a cookie policy that details what cookies are used, what information they collect and how this information is used. Users are asked to agree to the cookie policy when they access the site.

Those members of staff who are website administrators have their name and email address uploaded to the website appropriate to them. This is documented in the staff privacy notices.

The Privacy Notices relating to the use of student data are available on each school's website.

Confidentiality

The **Local Advisory Board of each school and the Board of Trustees** recognise that their members are in a privileged situation in that they have access to a great deal of information about the school, its pupils and staff. Members of the Local Advisory Board are reminded that any personal or sensitive information should remain private and should not be divulged verbally to anybody outside the remit of their role within the Local Advisory Board.

Our schools welcome **parent volunteers** to work alongside staff employed at the schools. In fulfilling this role such volunteers may become aware of sensitive information concerning an individual or group of pupils or even a member of staff. If this is the case, the volunteers are reminded that they should not repeat the information outside school or in the local community where access to it may be detrimental to the wellbeing or welfare of a pupil or member of staff.

Students undertaking **work experience** may find themselves in a similar situation and are reminded that they should retain a high level of confidentiality once outside the school environs.

Like Governors, **staff in all categories** find themselves in a privileged situation and will have access to large amounts of personal and confidential information. As part of their contract of employment, they are required to be discreet in terms of how such information is used. Information concerning pupils and other members of staff should only be used in the effective execution of their professional duties and under no circumstances divulged to people to whom it is not directly applicable. Care, in particular, will need to be made where the member of staff lives within the direct community served by the school.

Confidentiality policies will be sought from all contract cleaning companies, catering companies and supply teaching agencies.

Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our schools.
Our Primary and Infant Schools will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to the parent.
Our Secondary Schools will obtain written consent from parents/carers, or from students aged 13 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages
- Educational videos may be taken to improve teaching and learning.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.
When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Biometric Data

Biometric data is personal information about an individual's physical or behavioural characteristics that can be used to identify that person, including their fingerprints, facial shape, retina and iris patterns, and hand measurements. Where the Trust uses individuals' biometric data as part of an automated biometric recognition system (e.g. using pupils' fingerprints to receive school dinners instead of paying with cash), the school will comply with the requirements of the Protection of Freedoms Act 2012. Prior to any biometric recognition system being put in place, or processing biometric data, the Trust will obtain consent. Any individual (or the parent of a pupil aged under 18) can object to participation in the biometric system(s) or withdraw their consent at any time. Where this happens, any biometric data relating to the pupil that has already been captured will be deleted. The Trust will always endeavour to make available an alternative system which does not involve processing biometric data, for anyone who is not willing to consent.

In the case of pupils under the age of 18, parental consent will be required for biometric data processing. The parental consent form can be found in Appendix 7.

Subject Access Requests

Students, parents, staff and Governors have the right to ask to see a copy of any information we hold about them. This is known as a Subject Access Request (SAR).

To do this, they can write to any of our schools directly or email us at dataprotection@twynhamlearning.com. Subject Access Requests can only be taken in writing. If any members of staff receive a subject access request, they should pass it to the Data Protection Officer.

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our Primary or Infant Schools may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Students aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our Secondary School may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not disclose information if it:

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

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

Personal Data Breaches

All staff will receive training around what constitutes a data breach and will be asked to report any matters causing concern to dataprotection@twynhamlearning.com
The Data Protection Officer, once informed, will investigate the incident and evaluate the level of risk involved. An action plan will be formulated and shared with a member of the Leadership Team at the appropriate school. The Chief Executive Officer will also be informed. All breaches, whether or not they are reported to the ICO, will be recorded by the Data Protection Officer.

In cases where there is deemed to be a high risk to an individual's privacy, or the privacy of a group of people as a result of the breach, the Data Protection Officer will inform the ICO. The individuals concerned will also be informed.

Appendices

Appendix 1 – Twynham School Privacy Notice

Appendix 2 – Twynham School Staff Privacy Notice

Appendix 3 – Password Guidelines

Appendix 4 – Confidential Post Checklist

Appendix 5 – Guideline for giving out personal data over the telephone

Appendix 6 – Data Protection Assessment

Appendix 7 – Fingerprint Consent Form

Please note that the Privacy Notices are subject to change.

The distribution of the Staff Privacy Notice will be undertaken at each school in the means most appropriate to that site.

Appendix 1: Privacy Notice: How we use Student Information

We, Twynham School, are the data controller of the personal information you, or your previous school, provide to us. This means the school determines the purposes for which, and the manner in which, any personal data relating to students and their families is to be processed.

The categories of student information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information (such as Key Stage 1 and 2 scores, internal and external examination results)
- Medical information (such as allergies and existing medical conditions)
- Special Educational Needs information (such as results of testing and support strategies)
- Exclusions and Behaviour information (such as details of rewards, sanctions, detentions, suspensions)
- Post-16 destinations (education, employment, training)
- For Sixth Form students, the name of the school from which they joined us and their examination results
- Destinations of those students who leave before the normal leaving age, or mid-year

The lawful basis on which we collect and use this information

We collect and use personal data in order to meet legal requirements and legitimate interests set out in the GDPR and UK law, including those in relation to the following:

- Article 6 and Article 9 of the GDPR
- Education Act 1996
- Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013

Why we collect and use this information

In accordance with the regulations named above, we use student data:

- to support student learning
- to monitor and report on student progress
- to provide appropriate pastoral care
- to assess the quality of teaching and learning
- to comply with the law regarding data sharing
- to safeguard students

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

Storing student data

Personal data relating to students at Twynham School and their families is stored in line with the school's GDPR Data Protection Policy. In accordance with the GDPR, the school does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally collected.

Who we share student information with and why

We routinely share pupil information with schools that students attend after leaving us, our local authority (Dorset County Council), and the Department for Education (DfE). We are legally obliged to do this to comply with our census duties and in the case of other schools, to ensure data portability between schools. All data is transferred securely.

In addition, we regularly share student information with a number of organisations with the purposes of furthering teaching and learning and providing additional support and guidance to students. Our legal basis for doing this is that it is in the public interest and the interest of the students to enable them to access resources that will enhance their learning. The full list of organisations is available on our website at: www.twynhamschool.com/1437/privacy-notice.

Data collection requirements:

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

Data collection requirements:

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

Youth support services: Students aged 13+

Once our students reach the age of 13, we pass student 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 youth support services and careers advisers. Students can request that **only** their name, address and date of birth, as well as the name and address of their parent(s) is passed to their local authority or provider of youth support services by informing us. This right is transferred to the student once they reach the age of 13.

Youth support services: Students aged 16+

We will also share information about students 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 post-16 education and training providers, youth support services, and careers advisers. Students can request that **only** their name, address and date of birth, as well as the name and address of their parent(s) is passed to their local authority or provider of youth support services by informing us. This right is transferred to the student once they reach the age of 16.

For more information about services for young people, please visit the Dorset County Council website.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about students 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 students 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.

For more information about the NPD and how the DfE handles data, please see our extended Privacy Notice at: www.twynhamschool.com/1437/privacy-notice.

Your rights

You have the right to:

- Be informed about how we use your personal data.
- Request access to the personal data that we hold on you.
- Request that your personal data is amended if it is inaccurate or incomplete.
- Request that your personal data is erased where there is no compelling reason for its continued processing.
- Request that the processing of your data is restricted.
- Object to your personal data being processed.

Where the processing of your data is based on your consent (for example, photographic images), you have the right to withdraw this consent at any time.

Contact and Concerns

If you would like to discuss anything in this privacy notice, please contact the Data Protection Officer at Twynham Learning, Hannah Plane, by email at dataprotection@twynhamlearning.com.

If you have a concern about the way we and/or the DfE are collecting or using your personal data, you can raise a concern with the Information Commissioner's Office (ICO). The ICO can be contacted on 0303 123 1113, Monday-Friday 9am-5pm.

Appendix 2: Privacy Notice: How we use Staff Information

We, Twynham School, are the data controller of the personal information you provide to us. This means the school determines the purposes for which, and the manner in which, any personal data relating to staff is to be processed.

The categories of school workforce information that we collect, process, hold and share include:

- Personal information (such as name, employee or teacher number, national insurance number)
- Special categories of data including characteristics information such as gender, age, ethnic group
- Contract information (such as start dates, hours worked, post, roles and salary information)
- Work absence information (such as number of absences and reasons)
- Qualifications (and, where relevant, subjects taught)
- Salary information
- Medical information (for example allergies and existing medical conditions)
- Information about the vehicle that you drive
- Outcomes of any disciplinary procedures

The lawful basis on which we process this information

We collect and use personal data in order to meet legal requirements and legitimate interests set out in the GDPR and UK law, including those in relation to the following:

- Article 6 and Article 9 of the GDPR
- Education Act 1996

Why we collect and use this information

We use school workforce data to:

- Enable the development of a comprehensive picture of the workforce and how it is deployed
- Inform the development of recruitment and retention policies
- Enable individuals to be paid, and allow better financial modelling and planning
- Support the effective performance management of staff
- Enable us to contact staff whose vehicle has been involved in an accident or parked inappropriately
- Enable ethnicity and disability monitoring

Storing this information

Personal data relating to staff at Twynham School and their families is stored in line with the school's GDPR Data Protection Policy. In accordance with the GDPR, the school does not store personal data indefinitely; data is stored for as long as you work for us, and for three years after that.

Who we share staff information with and why

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.

In addition, we share staff information with the following organisations:

Name	Information shared	Reason
Capita SIMS	All information	SIMS is our Management Information System and houses all the information categories detailed above.
HR & Payroll Providers	Staff bank details and personal details	To allow all staff to be paid in line with their contract and to allow the build-up of a personnel record
EFSA	If appropriate and with your consent, staff details will be shared with these organisations. This may include personal details such as periods of sickness.	
Occupational Health		
Parents Evening System & Room Booking System	Name, email address, class codes, rooms.	Teaching staff details are uploaded to create accounts. This then gives staff access to the systems.
HCSS	Name and salary information	This is the school's budgeting tool. Salary information is used to allow the school to plan ahead for the year.

Depending on the department in which you work, staff details such as name and email address may also be uploaded to the following services in order to provide accounts:

- Access Reading Tests (Student Support)
- ActiveLearn and ActiveTeach (MFL)

- ALPS (Support Staff, SLT)
- Cleverbox (Website admins)
- FFT Aspire (Admin staff)
- Kerboodle (MFL, Science, History)
- Mathswatch (Maths)
- MyConcern (designated staff)
- MyMaths (Maths staff)
- SchoolComms (admin staff)
- Secure Testing for Schools (Student Support)
- SISRA
- Times Table Rockstars (Maths)

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 the 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

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact Hannah Plane on extension 277 or by email at hannah.plane@twynhamschool.com.

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

Contact and Concerns

If you would like to discuss anything in this privacy notice, please contact the Data Protection Officer at Twynham Learning, Hannah Plane, by email at hannah.plane@twynhamschool.com or by phone at 01202 486237.

If you have a concern about the way we and/or the DfE are collecting or using your personal data, you can raise a concern with the Information Commissioner's Office (ICO). The ICO can be contacted on 0303 123 1113, Monday-Friday 9am-5pm.

Appendix 3 - Password Guidelines

What would a student see if they were to log on to my account?

- Emails
- MIS data such as student home addresses, contact details, staff information, etc…
- Any files you keep on your account
- The contents of any shared drives or internal gateways
- Other staff-only sections of the network

Therefore, when using the Twynham Learning network and any associated device provided to you it is essential that you take the security of your personal account very seriously.

How do I choose a secure password?

Please use the following guidelines when setting your password:

- Over 8 characters long
- Meets 2 of the 3 conditions below:
  - Contains a number
  - Contains a mixture of uppercase and lowercase characters
  - Contains a special character

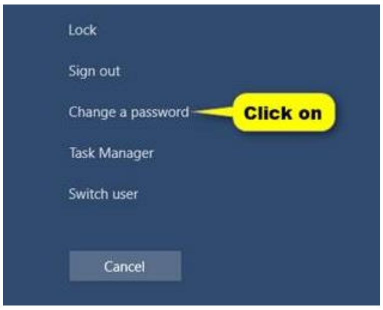
If your password does not comply with the above guidelines, please change it immediately.

If you have trouble creating a password simply think of two or more random capitalised words joined together and add a number to the end, for example "**TallFootballSocks95**". This makes the password easy to remember but also secure.

Please ensure you never set "123456", "Twynham", "rob123" etc. as your password.

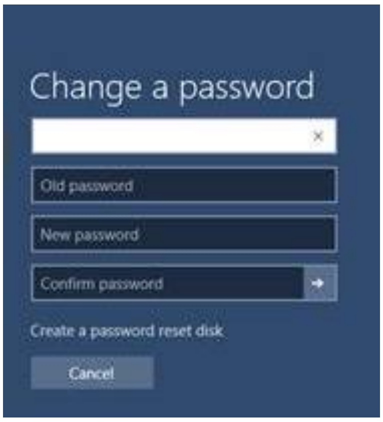
If you need any help at all, or think that your account may have been compromised, please contact IT Services.

How often should I change my password?



IT Services do not force you to change your password regularly so as not to interfere with teaching and learning or cause undue stress to staff. However, we do recommend that your review and change your password regularly, and especially in circumstances where you feel that your account may have been compromised.

How do I change my password?



Press CTRL, ALT and DELETE together while logged on to a device. The screen on the top left will appear.

Click on 'Change a password'.

Enter your old password in the correct box, and then a new password in the 'new password' and 'confirm password' boxes.

Click on the arrow to confirm your password change.

Twynham Learning

Appendix 4 - Confidential Post – Checklist

Sending out personal data by post is a potential source of data breaches. Information sent to the wrong address, or sent out without the contents being thoroughly checked, could allow personal data to be seen by people who have no reason to see it, or who should not be seeing it. Please use this form to ensure that you have carefully checked the contents, address details, and envelope.

Once completed, this form should be kept in a secure file, to be checked in the event of a postal data breach being discovered. Forms should be kept for a period of 3 months.

STATEMENT	TICK TO CONFIRM
There is a covering letter explaining the contents of the letter, and this is addressed to the correct person.	
Any additional content has been checked to ensure that it is the correct information to send to the named person.	
The address of the recipient is clearly visible through the envelope address window, or clearly written on the envelope.	
The envelope is marked 'Confidential; Addressee Only'.	
There is a return address clearly written or stamped on the envelope, in case the letter is not correctly delivered.	
If you are expecting data to be returned, you have included a stamped, addressed envelope, with sufficient postage, marked 'confidential'.	
The envelope is securely sealed.	

Recipient Name	
Name of person checking the letter	
Signed	
Date	

Appendix 5 – Telephone Requests for Data - Procedure

When dealing with a telephone call asking you to divulge the personal information, it is advisable to do so with the MIS open in front of you.

Procedure 1 - The caller says that they are a parent of a child and wishes to check where the child is, whether they have a club after school etc.

- Step 1
  Tell the caller that you need to verify their identity by asking them some questions. This needs to be things that only a parent would know, but that you have recorded in the MIS.

  Examples: What is the middle name of the child? What is their address? What class are they in? What is the child's date of birth? What are the names of their siblings?

- Step 2
  Check that the number they are calling from is one that you have for them on the MIS.

- Step 3
  Check that there are no notes in the MIS that tell you not to divulge information to this parent.

- Step 4
  Only divulge the information requested if you are satisfied on all of the above points.
  If there is any uncertainty, tell them that you will ring them back on the number that you have for them in the MIS in order to verify their identity.

Procedure 2 - The caller is not a parent but an agency who has links with a child (e.g. CAMHS) and wishes you to provide information about the child or their parents, e.g. contact details.

- Step 1
  Make a note of the details that they are asking for.
  Tell the caller that you will ring them back on the number that you have for them in the MIS and that this is because you need to verify their identity.

- Step 2
  Ring the caller back on the number that you have for them in the MIS.

- Step 3
  If the request is a double check on information that they have received from the parent, child, or yourself as a school, you may do this.
  If the request is to request new information about a student, they will need to email or write to the school to formally request this, and have the parents' permission to do so.
  If the request is regarding the parent, such as contact details, this is not your data to pass on to the agency. Do not divulge this information.

Appendix 6 - Data Protection Impact Assessment

These questions are intended to help you decide whether a DPIA is necessary. **Answering 'yes' to any of these questions is an indication that a DPIA would be a useful exercise**. You can expand on your answers as the project develops if you need to. You can adapt these questions to develop a screening method which fits more closely with the types of project you are likely to assess.

- 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?

Step one: Identify the need for a DPIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example a project proposal. Also summarise why the need for a DPIA was identified (this can draw on your answers to the screening questions).

Step two: 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.

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process. Consultation can be used at any stage of the DPIA process.

Step three: identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale DPIAs might record this information on a more formal risk register.

Privacy Issue	Risk to individuals	Compliance Risk	Associated organisation/corporate risk

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	Solution (s)	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?)

Step five: Sign off and record the DPIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by

Step six: Integrate the DPIA outcomes back into the project plan

Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action
Contact point for future privacy concerns:		

Linking the DPIA to the data protection principles

Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act.

Principle 1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
a) at least one of the conditions in Schedule 2 is met, and b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
Have you identified the purpose of the project?
How will individuals be told about the use of their personal data?
Do you need to amend your privacy notices?
Have you established which conditions for processing apply?
If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?
If your organisation is subject to the Human Rights Act, you also need to consider:

- Will your actions interfere with the right to privacy under Article 8?
- Have you identified the social need and aims of the project?
- Are your actions a proportionate response to the social need?

Principle 2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
Does your project plan cover all of the purposes for processing personal data?
Have potential new purposes been identified as the scope of the project expands?

Principle 3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
Is the information you are using of good enough quality for the purposes it is used for?
Which personal data could you not use, without compromising the needs of the project?

Principle 4 Personal data shall be accurate and, where necessary, kept up to date.
If you are procuring new software does it allow you to amend data when necessary?
How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5 Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.
What retention periods are suitable for the personal data you will be processing?
Are you procuring software which will allow you to delete information in line with your retention periods?

Principle 6 Personal data shall be processed in accordance with the rights of data subjects under this Act.
Will the systems you are putting in place allow you to respond to subject access requests more easily?
If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Principle 7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
Do any new systems provide protection against the security risks you have identified?
What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Principle 8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
Will the project require you to transfer data outside of the EEA? If you will be making transfers, how will you ensure that the data is adequately protected?

Fingerprint Consent Form

December 2018 saw us install a cashless catering system that has allowed us to provide a faster, more efficient catering service for our staff and students, and which has eliminated the need for students to carry cash or Free School Meals cards.

Since then, the school canteen has not accepted payments in cash.

Students are required to pay using a fingerprint or key fob.

In order for the cashless catering system to function, we are asking parents to provide consent for their child to have their fingerprint scanned. The fingerprint itself will not be stored; an algorithm will be made of it to be used only for the cashless catering system. The algorithm will be shared only with Nationwide Retail in order to link it to the correct student and Wisepay account.

Should you feel that you are unable to consent to fingerprint scanning, we will issue your child with a key fob that they will be able to swipe at the till.

Please complete the form below to indicate whether you consent to fingerprint scanning or whether you would prefer your child to receive a key fob.

You may change your mind regarding this consent at any time by writing to our Data Protection Officer at the address at the bottom of this letter or by emailing dataprotection@twynhamlearning.com.

Name of student: ____

□ I **consent** to my child's fingerprint being taken by Twynham School for the purpose of cashless catering.

□ I would prefer my child to receive a key fob.

□ I understand that I have the right to change my mind regarding this fingerprint at any time, and that I can do this by emailing dataprotection@twynhamlearning.com or by telephoning 01202 486237.

Signed: ______________________________ **Please print your name**: ____________________________________

Equality Impact Assessment – Initial Screening Record

1. What policy is being reviewed?	Data Protection Policy
2. Upon whom will this impact?	Everyone associated with Twynham Learning

3. How would the work impact upon groups; are they included and considered?

The Equality Strands	Negative impact	Positive impact	No impact
Minority ethnic groups			√
Gender			√
Disability			√
Religion, faith or belief			√
Sexual orientation			√
Transgender			√
Age (N/A to pre-school and school children)			√
Rurality			√

4. Does data inform this work, research and/or consultation, and has it been broken down by the equality strands?

	NO	YES	Uncertain
Minority ethnic groups	√		
Gender	√		
Disability	√		
Religion, Faith or belief	√		
Sexual Orientation	√		
Transgender	√		
Age	√		
Rurality	√		

Does the initial screening highlight potential issues that may be illegal? NO

Further comments:-

Do you consider that a full Equality Impact Assessment is required? NO

Initial screening carried out by Board of Trustees 27/06/18

Comment by CEO: