Toddington St. George C.E. School

Data Protection Policy

Edition 2: May 25 2018

Approved By: Governing Body

Document Control		
Edition	**Issued**	**Changes from previous**
1	1 Mar 16	None – new policy
2	1 June 18	To reflect GDPR

Policies/Documents referred to in this policy	Postholders/Persons named in this policy
Data Protection Act General Data Protection Regulations	Data Protection Controller Data Protection Officer

Review cycle: every 2 years
Review date: June 2020

Data Protection Policy

Vision

Toddington St George Church of England School (Diocese of St Albans) is an inclusive Christian community in which the curriculum is underpinned by agreed values based on Christian teaching.

The strategic plan, aims and policies enable every member of the school community to be valued as a child of God where they are given the opportunity to be inspired, challenged and supported in their learning and to receive committed, conscientious pastoral care.

This is embodied in the TSG school vision 'Lighting a Spark in Every Child'.

1.Introduction

The General Data Protection Regulations (GDPR), to be included in the expected Data Protection Act 2018, is the law that protects personal privacy and upholds individuals' rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the GDPR. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

The School is required to process relevant personal data regarding staff, students, their parents and guardians.

The school must manage and process personal data properly, protect the individual's right to privacy and provide an individual with access to all personal data held on them.

The school will make available privacy notices which inform data subjects why their personal information is needed, how it will be used and with whom it will be shared (see Appendix A)

2. The Principles

The school shall, so far as is reasonably practicable, comply with the six Data Protection Principles contained in the GDPR to ensure all data is:

i. Processed lawfully, fairly and in a transparent manner;

ii. Collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes;

iii. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

iv. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

v. 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;

vi. 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 and organisational measures.

3. Personal Data

Personal information is any information that relates to a living individual who can be identified from the information, including information such as an online identifier, such as an IP address. This includes both automated personal data and manual filing systems, as well as chronologically ordered data and pseudonymised data.

In the context of this document and the School's requirement to process "personal data" as part of its duty of care and to educate its students, "personal data" may include:

- Pupil records including name and address, date of birth, emergency contacts
- School admission and attendance registers
- Student's curricular records
- Reports to parents on the achievements of their children
- Records in connection with students entered for prescribed public examinations
- Student disciplinary records
- Personal information for teaching purposes
- Staff records, including payroll records
- References

In addition, the school may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities, Government Agencies and other bodies.

Personal data such as racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning health or data concerning a person's sexual orientation is classed as special categories of personal data, and the processing of this data is more strictly controlled.

4. Processing Personal Data and Consent

The school will only process personal data where one of the following applies:

i. the data subject has given consent;

ii. processing is necessary for the fulfilment of a contract in which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
iii. processing is necessary for compliance with a legal obligation to which the controller is subject;
iv. processing is necessary in order to protect the vital interests of the data subject or another natural person;
v. processing is necessary so that the school, as a public authority, can carry out a task in the public interest;
vi. processing is necessary for the purpose of the legitimate interests of the school or a third party

In general, the school processes pupil data so that it can carry out its duties as a public authority, and staff data is processed to fulfil the contract of employment we have with the member of staff. We will explain in our privacy notices the lawful basis for processing data, or ask for consent where one of the other bases does not apply.

For special categories of data, explicit consent to process the data will be required unless the processing is necessary for one of the special purposes listed in Article 9 of the GDPR.

5. Consent

Where processing is based on consent, the consent given will be a positive indication, rather than inferred. Requests for consent will be in an intelligible and easily accessible form, using clear and plain language. Under the GDPR, children under the age of 13 are not considered mature enough to give consent, so where we require consent to process data, we will request this from the child's parents.

6. Photography and video recordings

The school may take photographs or video footage of pupils within the school. These may be used internally on school noticeboards or in classrooms, or may appear externally in publications such as the prospectus, or on the school website or Facebook page. External agencies such as the school photographer may take photos, or photos may be made available to local newspapers. When photos are used externally, they will not be accompanied with any other personal information about the child. The school will obtain consent from parents (or the individuals if over 16) to use these images, and will explain how the photos will be used. Parents can refuse to give consent, or withdraw it at any time.

7. CCTV

We use CCTV cameras around the school to keep it safe. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose. We provide notices to make it clear that individuals are being recorded, and footage is destroyed after six months.

8. Data Protection Controller and Data Protection Officer

The school has a legal responsibility to comply with the GDPR. The school, as a corporate body, is named as the Data Controller under the Regulations.

Data Controllers are people or organisations who determine the purposes and means of the processing of personal data. The school is required to 'notify' the Information Commissioner that they are processing personal data. This information will be included in a public register which is available on the Information Commissioner's website:

https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

A Data Protection Officer (DPO) will be appointed to inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws, and to monitor the school's compliance with these laws. The DPO will have professional experience and knowledge of data protection law, will report to the highest level of management at the school and will operate independently. Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

9. Rights of Access

Individuals have a right of access to information held by the School. Any individual wishing to access their personal data should submit a Subject Access Request (SAR) in writing or by email addressed to the Data Protection Officer at the school address:

Data Protection Officer
Toddington St George CE School
Manor Road
Toddington
Bedfordshire
LU56AJ

toddstg@cbc.beds.sch.uk

Requests will be responded to within a month, unless there are numerous or complex requests, in which case the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary within one month of the receipt of the request. The school will verify the identity of the person making the request before any information is supplied.

Where a request is manifestly unfounded or excessive, the school retains the right to refuse to respond to the request. The individual will be informed of the decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

A copy of the information will be supplied to the individual free of charge, however the School may charge a reasonable fee for providing further copies of the same information, or where a request is manifestly unfounded, excessive or repetitive. All fees will be based on the administrative cost of providing the information.

10. Other rights of the individual

In addition to the rights to make a Subject Access Request, individuals also have the following rights:

- right to rectification of personal data held by the school
- right to erasure of personal data held by the school where there is no compelling reason for its continued processing
- right to restrict processing of their personal data by the school
- right to data portability, ie to request that their personal data is transferred to a third party in a structured, commonly used and machine-readable form
- right to object to the processing of personal data on the basis of legitimate interests or the performance of a task in the public interest, for the purposes of direct marketing or for purposes of scientific or historical research
- right to be notified of a data breach in certain circumstances

Any requests to exercise these rights should be addressed to the DPO at the address given above.

11. Data protection by design and default

The school will adopt a privacy by design approach, and implement technical and organisational measures which demonstrate how the school has considered and integrated data protection principles into all processing activities.

Privacy impact assessments (PIAs) will be used where the processing of data is likely to result in a high risk to the rights and freedoms of individuals, and when new technologies are introduced. The PIA will include a description of the process and its purpose, an assessment of the necessity and proportionality of the processing in relation to the purpose, an outline of the risks to individuals and the measures implemented to address the risk.

The school will provide comprehensive, clear and transparent policies and privacy notices, and only process data that is necessary for each specific processing purpose.

12. Data Security

The school will determine and maintain an appropriate level of security and back up for its premises, equipment, network, programs, data and documentation, and will ensure that access to them is restricted to appropriate staff. In particular:

- **Paper-based records** are kept in locked filing cabinets or cupboards, with restricted access
- **Confidential paper records** will not be left unattended or in clear view anywhere with general access
- Where **paper ,computer files or other memory sticks with files** need to be taken off site, these must be **signed in and out** of the Trust office (at the school in question)
- **Digital data is coded, encrypted or password-protected**
- Where data is saved on **removable storage or a portable device**, the device is kept in a locked cabinet, drawer or safe when not in use

- **Memory sticks** will not be used to hold personal data unless they are password-protected and fully encrypted
- **All electronic devices** are password-protected to protect the information in case of theft
- Governors who use personal devices are expected to follow the same security procedures as for school owned equipment
- **Staff will not use their personal laptops or computers for school purposes**
- Where data is transferred to another data processor (eg payroll provider), the school has obtained confirmation that they are storing and processing the data in accordance with GDPR

13. Data Breaches

The school will take all reasonable steps to ensure that there are no data breaches, but if one does occur, the following steps will be taken:

- On finding a potential data breach, the relevant party must inform the DPO immediately
- The DPO will consider whether a breach has occurred, ie has data been lost, stolen, destroyed, altered, disclosed when it should not have been, or made available to unauthorised people
- The DPO will assess the risk of the breach having a detrimental effect on the individual or causing them damage, and decide whether the breach must be reported to the ICO.
- If reporting is considered necessary, this will be done within 72 hours of the breach, and will document the nature of the breach, with categories and numbers of individuals and/or records concerned, an explanation of the likely consequences, and a description of the measures taken to mitigate any adverse effects
- If the risk to individuals is high, then the DPO will also notify all individuals concerned, with the same information as above.

14. Disposal of records

Data will not be kept for longer than is necessary – retention periods are detailed in Appendix B.

Unrequired data will be deleted as soon as practicable.

Paper documents will be shredded and electronic files overwritten or deleted.

We may also use a third party to dispose of records on our behalf, and will obtain guarantees for them that they comply with GDPR.

Appendix A i – Privacy Notice for pupils

Privacy Notice (How we use pupil information)

The categories of pupil 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
- Relevant medical information
- Special educational needs information
- Exclusions/behavioural information

Why we collect and use this information

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing

The lawful basis on which we use this information

We collect and use pupil information under Article 6e (task in the public interest) and Article 9 (consent) for special category data from the GDPR.

Collecting student 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 General Data Protection Regulation, 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 25 years from the date of birth of the student *[for upper schools]* / for the time they attend our school, after which their file is passed on to their next school *[for lowers/middles].* Safeguarding information may be retained for a longer period.

Who we share pupil information with

We routinely share pupil information with:

- schools that the pupils attend after leaving us
- our local authority
- the Department for Education (DfE)
- the NHS where appropriate

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 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.

The National Student 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 DPO on the address above.

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, we request that you raise your concern with us in the first instance. Alternatively, you can contact 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:

Data Protection Officer
c/o Toddington St George CE School
Manor Road
Toddington
Bedfordshire
LU56AJ

office@toddstg.co.uk

Appendix A ii – Privacy Notice for School Workforce

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)

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

The lawful basis on which we process this information

We process this information under Article 6 1b because it is necessary for the performance of the contract we have with you, to ensure that you are paid correctly and the correct deductions are made for tax, national insurance and pensions. Also, sensitive data is collected under Article 9 2b, because the processing is necessary for the purposes of carrying out our obligations in the field of employment, social security and social protection law.

We are also required to collect data for the school workforce census under the Education Act 1996 – see guidance at https://www.gov.uk/education/data-collection-and-censuses-for-schools

Collecting this information

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

Storing this information

We hold school workforce data for six years after termination of your employment, after which it is securely destroyed.

Who we share this information with

We routinely share this information with:

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

Why we share school workforce information

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority

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.

Department for Education (DfE)

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

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

Data collection requirements

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

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

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

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

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

- who is requesting the data

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

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

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

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

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

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 the DPO on the address above.

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, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Further information

If you would like to discuss anything in this privacy notice, please contact:

Data Protection Officer
c/o Toddington St George CE School
Manor Road
Toddington
Bedfordshire
LU56AJ

office@toddstg.co.uk

Appendix 2 – Retention of Documents

This schedule lists the principal documents held relating to pupils and staff, but is not an exhaustive list. For retention periods for other documents, please refer to the Information Management Toolkit for Schools – www.irms.org.uk

Document	**Period of retention**
Pupil-related records:	
Pupil file (electronic and paper copy) Lower/middle schools Upper school	 While the child remains at the school, then transferred to the next school Date of birth of pupil + 25 years
Child protection files	Date of birth of pupil + 25 years, then review
Attendance registers	3 years from date entry made
SEN files	Date of birth of pupil + 25 years
Examination results	Current year + 6 years
Parental consent forms for school trips	Conclusion of trip, unless major incident, in which case DOB of pupil involved + 25 years – all consent forms to be kept in this case, to show rules followed for all pupils
Staff related documents:	
Records leading up to appointment of a new member of staff – unsuccessful candidates - successful candidates	Date of appointment of successful candidate + 6 months Added to staff personal file (see below)
Staff personal file (electronic and paper copy)	Termination of employment + 6 years
Timesheets	Current year + 6 years
Annual appraisal/assessment records	Current year + 5 years
Allegations of child protection nature (even if unfounded)	Normal date of retirement or 10 years from date of allegation, whichever is longer

Disciplinary proceedings: - oral warning - written warning level 1 - written warning level 2 - final warning - case not found	 Date of warning + 6 months Date of warning + 6 months Date of warning + 12 months Date of warning + 18 months Dispose of at conclusion of case