

Policy: Data Protection (GDPR compliant)

Ratified FGB: July 2026

Review: July 2028

Holy Trinity Church of England (VA) Primary School



Believe • Achieve • Inspire •

Data Protection (GDPR Compliant) Policy

SCHOOL VISION

Our vision is for our pupils to flourish in an inclusive, inspirational place of learning where we are happy, respectful, kind and safe.

At Holy Trinity Church of England Primary School our Christian vision shapes all we do.

*"I know that there is nothing better for people than to be happy and to do good while they live."
Ecclesiastes 3:12.*

- we facilitate opportunities so every child can flourish in a place where they feel **safe, happy and confident**.
- staff **well-being** and professional development is valued and supported in order to fulfil their roles, **inspire** others and experience personal **fulfilment**.
- the school provides facilities that enables our pupils to reach their potential in an **optimum learning environment**.
- the **school plays a central role within our community** and enjoys strong **links with the church, local companies and other schools**.
- we create a culture of vigilance to **safeguard** all children.

'I know that there is nothing better for people than to be happy and to do good while they live.' Ecclesiastes 3:12

1. This policy covers all other school policies in regard to the protection of data.

2. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

3. Legislation & Guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

4. Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Religious or philosophical beliefs • Trade union membership • Genetics • Health – physical or mental • Sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

'I know that there is nothing better for people than to be happy and to do good while they live.' Ecclesiastes 3:12

Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
----------------------	---

5. The Data Controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

6. Roles & Responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Governing Board

The Governing Board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description. Our DPO's contact details are below:

Samantha Wootton
Data Protection Officer
Royal Borough of Windsor and Maidenhead
Town Hall
St Ives Road
Maidenhead SL6 1RF
01628 796338

email: DPO@rbwm.gov.uk

samantha.wootton@rbwm.gov.uk

Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis.

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address

'I know that there is nothing better for people than to be happy and to do good while they live.' Ecclesiastes 3:12

- Contacting the DPO in the following circumstances:
 - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
 - If they have any concerns that this policy is not being followed
 - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
 - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
 - If there has been a data breach
 - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
 - If they need help with any contracts or sharing personal data with third parties

7. Data Protection Principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

8. Collecting Personal Data

a. Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carers when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

'I know that there is nothing better for people than to be happy and to do good while they live.' Ecclesiastes 3:12

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

b. Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Information and Records Management Society's toolkit for schools. (See Data Retention Policy).

9. Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carers that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
 - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
 - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
 - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

10. Subject Access Requests and other Rights of Individuals

a. Subject access requests

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

- Confirmation that their personal data is being processed

'I know that there is nothing better for people than to be happy and to do good while they live.' Ecclesiastes 3:12

- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the Headteacher and DPO.

b. Children and subject access requests

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 school 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.

c. Responding to subject access requests

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.

d. Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

11. Parental requests to see Educational Record

The Governing Board gives the right for parental access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

12. CCTV

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras, if installed, will be clearly visible and accompanied by prominent signs explaining that CCTV is in use.

13. Photographs & Videos

As part of our school activities, we may take photographs and record images of individuals within our school.

Pupils aged under 18 years of age

We 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 both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, competition results etc.
- Online on our school website or social media pages

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.

'I know that there is nothing better for people than to be happy and to do good while they live.' Ecclesiastes 3:12

When using photographs and videos in this way we will only accompany them with their first name and not accompany them with any other personal information about the child, to ensure they cannot be fully identified.

See our Child Protection and Safeguarding Policy for more information on our use of photographs and videos.

14. Data Protection by Design & Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
 - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data Security & Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and tablets where personal information is stored

***'I know that there is nothing better for people than to be happy and to do good while they live.'* Ecclesiastes 3:12**

- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our E-Safety policy on acceptable use)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

16. Disposal of Records

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.

17. Personal Data Breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

18. Training

All staff and governors are provided with data protection training as part of their induction process. This is also referred to in the school staff induction handbook.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19. Monitoring Arrangements

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full Governing Board.

20. Links with Other Documentation

This data protection policy is linked to other school documents including:

- Freedom of information policy (Including publication scheme)
- Online Safety Policy and Acceptable Use
- Safeguarding and Child Protection Policy
- Data Retention policy
- Staff Induction Handbook
- Equality Act 2010

'I know that there is nothing better for people than to be happy and to do good while they live.' Ecclesiastes 3:12

In reviewing this policy, the Governing Board has had regard to the Equality Act 2010 and carried out an equality impact assessment. It is satisfied that no group with a protected characteristic will be unfairly disadvantaged by this policy.

This policy was adopted by Holy Trinity CE Primary School and agreed and ratified by the Full Governing Board.

Approved by.....on behalf of the School Governing Board.

Signature:.....

Date:.....

Appendix 1 – Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
- The DPO will alert the headteacher and the Chair of Governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
 - Loss of control over their data
 - Discrimination
 - Identify theft or fraud
 - Financial loss
 - Unauthorised reversal of pseudonymisation (for example, key-coding)
 - Damage to reputation
 - Loss of confidentiality
 - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored by the DPO on the Trust's central systems.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

'I know that there is nothing better for people than to be happy and to do good while they live.' Ecclesiastes 3:12

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored by the DPO on the Trust's central systems.

- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted. Other types of breach that you might want to consider could include:
 - Details of pupil premium interventions for named children being published on the school website
 - Non-anonymised pupil exam results or staff pay information being shared with governors
 - A school laptop containing non-encrypted sensitive personal data being stolen or hacked
 - The school's cashless payment provider being hacked and parents' financial details stolen

'I know that there is nothing better for people than to be happy and to do good while they live.' Ecclesiastes 3:12

Transferring data internationally

Where we share data with an organisation that is based outside the European Economic Area, we will protect your data by following data protection law.

Your rights

a. How to access personal information we hold about you

You can find out if we hold any personal information about you, and how we use it, by making a **'subject access request'**, as long as we judge that you can properly understand your rights and what they mean.

If we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and using it, and how long we will keep it for
- Explain where we got it from, if not from you or your parents
- Tell you who it has been, or will be, shared with
- Let you know if we are using your data to make any automated decisions (decisions being taken by a computer or machine, rather than by a person)
- Give you a copy of the information

You may also ask us to send your personal information to another organisation electronically in certain circumstances.

If you want to make a request please contact our data protection officer.

GDPR Privacy Notice – Pupils and Families

Who processes your information?

Holy Trinity CE Primary School, Sunningdale (hereafter Holy Trinity School or school) is 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 pupils and their families is to be processed.

In some cases, your data will be outsourced to a third party processor; however, this will only be done with your consent, unless the law requires the school to share your data. Where the school outsources data to a third party processor, the same data protection standards that Holy Trinity School upholds are imposed on the processor.

The local authority, RBWM, has a nominated data protection officer (DPO) who acts on behalf of the school. Their role is to oversee and monitor the school's data protection procedures, and to ensure they are compliant with the GDPR. The data protection officer can be contacted via the school office.

Why do we collect and use your information?

Holy Trinity School holds the legal right to collect and use personal data relating to pupils and their families, and we may also receive information regarding them from their previous school, local authority and/or the Department for Education (DfE). 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

In accordance with the above, the personal data of pupils and their families is collected and used for the following reasons:

***'I know that there is nothing better for people than to be happy and to do good while they live.'* Ecclesiastes 3:12**

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our service
- to comply with the law regarding data sharing
- to safeguard pupils
- to fulfil legal and contractual obligations where otherwise reasonably necessary for school purposes.

Which data is collected?

The categories of pupil information that the school collects, holds and shares include the following:

- personal information – e.g. names, pupil numbers and addresses
- characteristics – e.g. ethnicity, language, nationality, country of birth and free school meal eligibility
- attendance information – e.g. number of absences and absence reasons
- assessment information – e.g. national curriculum assessment results
- relevant medical information
- information relating to SEND (Special Educational Needs and Disabilities)
- behavioural information – e.g. number of temporary exclusions
- images of students engaged in school activities and for identification purposes.

Whilst the majority of the personal data you provide to the school is mandatory, some is provided on a voluntary basis. When collecting data, the school will inform you whether you are required to provide this data or if your consent is needed. Where consent is required, the school will provide you with specific and explicit information with regards to the reasons the data is being collected and how the data will be used.

How long is your data stored for?

Personal data relating to pupils at Holy Trinity School and their families is stored in line with the school's GDPR Data Retention 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.

Will my information be shared?

The school is required to share pupils' data with the DfE on a statutory basis. This data underpins school funding and educational attainment policy and monitoring.

The National Pupil Database (NPD) is managed by the DfE and contains information about pupils in schools in England. Holy Trinity School is required by law to provide information about our pupils to the DfE as part of statutory data collections, such as the school census; some of this information is then stored in the NPD. The DfE may share information about our pupils from the NDP with third parties who promote the education or wellbeing of children in England by:

- Conducting research or analysis.
- Producing statistics.
- Providing information, advice or guidance.

The DfE has robust processes in place to ensure the confidentiality of any data shared from the NDP is maintained.

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

Holy Trinity School will not share your personal information with any third parties without your consent, unless the law allows us to do so. The school routinely shares pupils' information with:

- schools that the pupils attend after leaving us
- the NHS and School Nurse Team
- the Department for Education
- the LA, who under strict information sharing protocols and policies, may be required to share this information with other public sector partners such as other Local Authorities
- Wilson Jones, school catering partner and their lunch ordering partner, Biostore
- other compliant, third party providers to enhance student learning or education as approved by the Governing Board (e.g. Mathletics, Spellodrome, Purple Mash, Library Systems etc)
- Tapestry - EYFS assessment tool

'I know that there is nothing better for people than to be happy and to do good while they live.' Ecclesiastes 3:12

- other compliant third party providers in order to communicate effectively with families (e.g. Primary Site, Primary Contact etc)
- the Police when part of an investigation. All requests will be referred to the Headteacher or their representative.

For a full list of third party providers please contact the school.

In addition to this, pupil information will be provided to:

- OFSTED to help inspectors to evaluate schools
- Fischer Family Trust (FFT) for subject level analysis compared to previous years

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) under Section 3 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 go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>

What are your rights?

Parents and pupils have the following rights in relation to the processing of their personal data.

You have the right to:

- be informed about how Holy Trinity School uses your personal data
- request access to the personal data that Holy Trinity School holds
- 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, you have the right to withdraw this consent at any time.

If you have a concern about the way Holy Trinity School and/or the DfE store and use 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.

Where can you find out more information?

If you would like to find out more information about how we and/or the DfE collect, use and store your personal data, please visit our website www.holytrinityschsunningdale.co.uk to view our GDPR Data Protection Policy.

Transferring data internationally

Where we share data with an organisation that is based outside the European Economic Area, we will protect your data by following data protection law.

Your rights

How to access personal information we hold about you

You can find out if we hold any personal information about you, and how we use it, by making a 'subject access request' (SAR), as long as we judge that you can properly understand your rights and what they mean. If we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and using it, and how long we will keep it for
- Explain where we got it from, if not from you or your parents
- Tell you who it has been, or will be, shared with
- Let you know if we are using your data to make any automated decisions (decisions being taken by a computer or machine, rather than by a person)
- Give you a copy of the information

'I know that there is nothing better for people than to be happy and to do good while they live.' Ecclesiastes 3:12

You may also ask us to send your personal information to another organisation electronically in certain circumstances. If you want to make a request please contact the school office who will forward to the Headteacher for processing.

Privacy Notice – HR and Payroll Services - RBWM

Privacy Notice – This notice explains when we collect personal data, what we use it for, who we share it with and your rights.

Who are we – HR, Town Hall, St Ives Road, Maidenhead, SL6 1RF

The lawful basis for processing the information

All HR services operate within legislation detailed in Appendix A.

How do we collect information from you?

Data is collected via:

HR

- Job application forms submitted online, by email, post.
- HR forms submitted by new and current employees and managers – email and hard copy.
- HR forms submitted by schools – email and hard copy.
- Agency – pro-forma containing worker information via 3rd party online system or email form for off-framework agencies.
- Data gained during the processing of DBS applications – online and hard copy.
- Information gained during the management of employment processes – emails, letters, notes of interviews and meetings, reports - hard copy and electronic.
- Occupational health referrals – online form.
- Personal data is supplied by the employees via an online system supplied by third parties delivering various employee benefits.
- Verbally from employees to confirm identity when calling HR with personal queries.

Payroll

- Personal data is supplied by the individual employee via on line forms, emails, paper documents including bank account details, P45's, pensions history, union membership.
- Personal data is supplied via third parties electronically and/or hard copy – pension providers, AVC provider, HMRC, HM Courts and Tribunal Service, Contributions Agency, the council's employee benefits providers including Sodexo and NHS Fleet Solutions, trade unions - GMB and Unison.
- iTrent HR system- absences, overtime, expenses/mileage claims.
- HMRC notifications are uploaded directly into the HR system.

Health and Safety

- On line accident / incident report forms.
- Paper forms sent by schools and internal council services.

Learning and Development

Learning and development software system.

Email – learninganddevelopment@rbwm.gov.uk.

Quality Matters <https://www.learningpool.com/>

iHasco <https://app.ihasco.co.uk/client/login>

'I know that there is nothing better for people than to be happy and to do good while they live.' Ecclesiastes 3:12

What type of information is collected from you?

HR

- Personal details including names, addresses, date of birth, qualifications, examinations, career history, skills, experience etc.
- Emergency contacts
- Equalities data – the nine protected characteristics - age, sex, race, disability, gender reassignment, pregnancy/maternity, marriage/civil partnership, religion/belief and sexual orientation.
- Criminal convictions and cautions.
- Information regarding employment processes and procedures such as discipline, grievance, capability, ill health.
- Sickness absence dates and reasons.
- Health and absence information.

Payroll

- Date of marriage, NI number, personal bank account number, tax code, AVC payment value, salary sacrifice benefit value, value of official deductions including union subscriptions, court order payments, jury service payments etc.
- Monthly variable data including overtime hours, standby claims, mileage and other expenses.
- Maternity and other family related absence dates.

Health and Safety

- Full name, personal address, telephone number, date of birth, gender.
- Details of accident / incident and resulting injuries.
- Details of First aid treatment given.

Learning and Development

- Full name.
- Email address.

How we use the information you have provided

HR

- Application forms – to assess applicants for shortlisting and appointment and to determine suitability for employment at the outset and ongoing.
- Contact details - to communicate with employees.
- Employment records – respond to queries, record employment history.
- Pay data – to enable processing of salary and other payments.
- Pensions – for enrolment.
- To manage employees through the employee lifecycle – joining, probation, employment history, job transfers, processes such as capability, disciplinary, absence management, restructuring, salary changes, retirement, termination, transfer to other organisations.
- Equalities data – used to create a profile of the organisation.
- To assess the employees' application for specific benefits e.g. childcare vouchers.
- To confirm identity.
- Workforce monitoring and statistical analysis, including statutory workforce returns.
- Performance management.

'I know that there is nothing better for people than to be happy and to do good while they live.' Ecclesiastes 3:12

Payroll

- All associated payroll processing including payments for various absences.
- Pension scheme contribution and entitlements administration.
- Managing all calculations and processing of statutory and voluntary deductions from pay.

Health and Safety

- Accident Investigation and reports.

Learning and Development

- For the individual's record of learning.
- To analyse attendance and future course planning.

iTrent

- For administering the HR information system, validating data, reporting, development of functionality and testing new releases.

Who has access to the information about you?

HR

- HR Business Partner team, HR Strategic team for all HR processes before and during and after employment and for data validation, issue resolution and statistical purposes.
- HR Strategic team, HR Business Partner team and Payroll team for assessment, administration and overall management of pay and benefit schemes.

Payroll

- Payroll team in order to legally and accurately process payroll.

Health and Safety

- Health and Safety Advisors to allow for investigation of accidents, complete reports and benchmarking against other councils.

Learning and Development

- Learning and Development team to retain record of learning and manage learning events.

iTrent Systems team

- iTrent Systems team has access to all systems and data,

All HR teams

- Agency workers/consultants appointed to work within HR in order to undertake relevant HR service related activities.

Who we may share your information with

HR

- 3rd party occupational health services provider <http://www.ohworks.co.uk/>
- Organisations providing services for pre-employment checks:
- Disclosure & Barring Service <https://www.gov.uk/government/organisations/disclosure-and-barring-service>

'I know that there is nothing better for people than to be happy and to do good while they live.' Ecclesiastes 3:12

- Atlantic Data <http://www.atlanticdata.co.uk/>
- Thames Valley Police – safeguarding issues/criminal activity <https://www.thamesvalley.police.uk/>
- National College of Teaching & Leadership - part of statutory pre-employment checks before and during employment. And during inspections to demonstrate compliance with employment practices and referrals where there is concern about professional conduct.
performance. <https://www.gov.uk/government/organisations/national-college-for-teaching-and-leadership>
- 3rd party organisations in any TUPE transfer process - personal data will need to transfer to new employer.
- Pension providers - Berkshire Pension Fund (BPF) for the Local Government Pension Scheme (LGPS) <http://www.berkshirerpensions.org.uk/>
- Teachers Pensions Scheme <https://www.teacherspensions.co.uk/>
- NHS pension <https://www.nhsbsa.nhs.uk/>
- i-Connect – software for transferring LGPS data to the BPF <https://www.iconnectdata.co.uk/>
- Regulatory bodies –
- Ofsted <https://www.gov.uk/government/organisations/ofsted>
- Care Quality Commission <http://www.cqc.org.uk/>
- Health and Care Professionals Council <http://hpc-uk.org/>
- All internal service areas including schools/relevant managers - where information relates to their employees.
- 3rd party employee benefits service provider <https://uk.sodexo.com/home.html>
- 3rd party lease car scheme provider - <https://nhsfleetsolutions.co.uk/>
- Recognised Trade Unions - to meet statutory consultation requirements related to organisational change/TUPE processes
- <https://www.unison.org.uk/>
- <https://www.gmb.org.uk/>
- <http://www.naht.org.uk/>
- <https://neu.org.uk/>
- <https://www.ascl.org.uk/>
- 3rd party provider of on line job application system, JGP <https://www.jobsgopublic.com/>
- 3rd party provider – supplier of temporary agency workers, de Poel <https://www.depoel.co.uk/>
- 3rd party eye test voucher provider – Specsavers <https://www.specsavers.co.uk/>
- Various 3rd parties requesting references or continuous service date confirmation etc
- RBWM's internal and external audit service - to ensure compliance with internal controls and external regulations.
- RBWM's external Legal Services provider – Shared Legal Services (SLS - legal services at Wokingham Borough Council)
- For Employment Tribunal cases – Counsel will be commissioned via SLS.

Payroll

- Pension providers – LGPS administered by Berkshire Pension Fund, TPS, NHS- see above, Prudential – AVC provider - 3rd party for administration of contributions and payment of pension benefits. I-Connect – third party software provider for data transfer to the Berkshire Pension Fund.
- <https://www.pru.co.uk/rz/localgov/>
- For processing of payroll deductions -
- HMRC <https://www.gov.uk/government/organisations/hm-revenue-customs>
- DWP <https://www.gov.uk/government/organisations/department-for-work-pensions>
- HM Courts and Tribunal Service- for processing deductions <https://www.justice-ni.gov.uk/topics/courts-and-tribunals>
- Various 3rd parties requesting earnings confirmation for mortgages, loans etc
- RBWM's internal and external audit service - to ensure compliance with internal controls and external regulations.
- RBWM's Finance service - for financial processing/budget management.
- Trade Unions - check off information for union members, see above.

'I know that there is nothing better for people than to be happy and to do good while they live.' Ecclesiastes 3:12

Health and Safety

- Health and Safety Executive - where it is a requirement under RIDDOR Regulations <http://www.hse.gov.uk/>
- Line Managers including schools- accident details will be shared and discussed with the employee's line manager or supervisor.
- Council's Insurance Manager and insurers - to manage litigation and comply with insurance conditions.

Learning and Development

- 3rd party provider of the learning and development software system to enable management of learning records:
- Quality Matters <https://www.learningpool.com/>
- iHasco <https://app.ihasco.co.uk/client/login>
- Skillsoft <https://is023.skillport.com/skillportfe/login.action>
- Individually commissioned 3rd party training providers.

iTrent systems team

- RBWM ICT service desk - as necessary as part of HR help desk function.
- RBWM schools - the organisation collects data for and on behalf of schools as the employer which may be required by the individual schools for the purposes of reporting and budget monitoring at a school level.
- RBWM's Finance service - for the purpose of pay modelling and budgeting.
- Office of National Statistics - to satisfy the requirements of statutory returns. This is mostly anonymised but may include individual details <https://www.ons.gov.uk/>
- 3rd party HR system software provider - are given access to our database for; helpdesk call resolution, issue resolution, system development consultancy and reporting <https://www.mhr.co.uk/>
- [3rd party software used by Payroll – iConnect, Learning and Development – Quality Matters](#)
- National Fraud Initiative - in order to identify cross organisational fraud. Covers areas such as multiple employments, those in receipt of pension and salary, those in receipt of benefits and salary etc <https://www.nfi.gov.uk/>

How long we store your information

HR

- Unsuccessful job applicants – 6 months.
- Employment records – 7* years after termination of employment (6 tax years plus current tax year) in electronic document management system, plus word, and PDF documents on secure network.
- Employee pay and benefits records – 7* years after termination of employment in word, excel and PDF documents on secure network.

Payroll

- All payroll related records – 7* years after termination of employment. Electronically within Payroll system, excel/word documents on secure network.
- Associated pension records - 10 years after change. Electronically within Payroll system, excel/word documents on secure network.
- Overtime and other monthly claims from schools - 6 years after termination of employment. Hard copies – secure storage.

Health and Safety

- Accident records including RIDDOR– 3* years or where a child, until age 21. COSHH – 40 years.

'I know that there is nothing better for people than to be happy and to do good while they live.' Ecclesiastes 3:12

Learning and Development

- Record of learning 7# years after course completed or person leaves organisation. On eLearning software system.

iTrent Systems team

- Emails to help desk - personal information. Until the Call is resolved + plus 12 month for monitoring of issues. Outlook email / shared inbox & Excel Spreadsheet on secure network.
- Phone calls to help desk – personal. Until the Call is resolved + plus 12 months for monitoring of issues. Excel Spreadsheet on secure network.

* For those working with children, 25 years.

For those working with children 40 years.

Does your service utilise automate decision making? – No.

Appendix A – Lawful Basis for Processing Personal Information

All HR services operate within the following legislation:

HR

ACAS Arbitration Scheme (England and Wales) Order 2001.
ACAS Arbitration Scheme (Great Britain) Order 2004.
Access to Medical Reports Act 1988.
Acquired Rights Directive (2001/23/EC).
Agency Workers Regulations 2010.
Apprenticeships, Skills, Children and Learning Act 2009.
Asylum and Immigration Act 1996 and 1999.
Bribery Act 2010.
Care Standards Act 2000.
Collective Redundancies Directive (75/129/EC).
Collective Redundancies (Amendment) Regulations 2006.
Collective Redundancies and Transfer of Undertakings (Protection of Employment) (Amendment) Regulations 1995, 1999 and 2014.
Conduct of Employment Agencies and Employment Businesses Regulations 2003.
Criminal Justice and Court Services Act 2000.
Disability Discrimination Act 1995, 2005.
Education and Skills Act 2008.
Employee Study and Training (Eligibility, Complaints and Remedies) Regulations 2010.
Employee Study and Training (Procedural Requirements) Regulations 2010.
Employment Act 2002 and 2008.
Employment Equality (Age) Regulations 2006.
Employment Equality (Age) (Amendment No.2) Regulations 2006.
Employment Equality (Religion or Belief) Regulations 2003.
Employment Equality (Repeal of Retirement Age Provisions) Regulations 2011.
Employment Equality (Sex Discrimination) Regulations 2005.
Employment Equality (Sexual Orientation) Regulations 2003.
Employment Relations Act 1999 and 2004.
Employment Relations Act 1999 (Blacklists) Regulations 2010
Employment Rights Act 1996.
Employment Rights Act 1996 (Application of Section 80B to Adoptions from Overseas) Regulations 2003.
Employment Tribunals Act 1996.
Employment Tribunals (Constitution and Rules of Procedure) Regulations 2013. Employment Tribunals (Early Conciliation: Exemptions and Rules of Procedure) Regulations 2014.
Equality Act 2010.
Equality Act (Age Exceptions for Pension Schemes) Order 2010.
Equality Act 2010 (Gender Pay Gap Information) Regulations 2017.
Equality Act 2010 (Obtaining Information) Order 2010.
Equality Act 2010 (Specific Duties and Public Authorities) Regulations 2017.
Equality Act 2010 (Sex Equality Rule) (Exceptions) Regulations 2010.
Equal Opportunities and Equal Treatment Directive (2006/54/EC).
Equal Pay Act 1970.
Equal Treatment Framework Directive (2000/78/EC).
Exclusivity Terms in Zero Hours Contracts (Redress) Regulations 2015.
Finance Act 2009, 2011, 2013, 2016 and 2017.
Fixed-term Workers Directive (99/70/EC).
Fixed-Term Employees (Prevention of Less Favourable Treatment) Regulations 2002.
Flexible Working Regulations 2014.
Gender Recognition Act 2004.
Human Rights Act 1998.
Immigration Act 2014.
Immigration, Asylum and Nationality Act 2006.
Immigration (Restrictions on Employment) Order 2004 and 2007.
Information and Consultation Directive (2002/14/EC).

'I know that there is nothing better for people than to be happy and to do good while they live.' Ecclesiastes 3:12

Information and Consultation of Employees Regulations 2004.
 Maternity and Adoption Leave (Curtailment of Statutory Rights to Leave) Regulations 2014.
 Maternity and Parental Leave etc. Regulations 1999.
 Maternity and Parental Leave (Amendment) Regulations 2001.
 Maternity and Parental Leave etc. and the Paternity and Adoption Leave. (Amendment) Regulations 2006 and 2008.
 The Maternity and Parental Leave etc. (Amendment) Regulations 2014.
 National Minimum Wage Act 1998.
 National Minimum Wage (Amendment) Regulations 2016 and 2017.
 National Minimum Wage (Enforcement Notices) Act 2003.
 National Minimum Wage Regulations 2015.
 Part-time Workers Directive (97/81/EC).
 Part time workers (Prevention of Less Favourable Treatment) Regulations 2000.
 Parental Leave Directive (2010/18/EC).
 Paternity and Adoption Leave Regulations 2002.
 Paternity and Adoption Leave (Adoption from Overseas) Regulations 2003.
 Paternity and Adoption Leave (Amendment) Regulations 2004 and 2014.
 Social Security (Paternity and Adoption) Amendment Regulations 2002
 Pensions Act 1995, 2004, 2007, 2011, 2014.
 Pension Schemes Act 2015.
 Occupational and Personal Pension Schemes (Consultation by Employers and Miscellaneous Amendment) Regulations 2006.
 Occupational and Personal Pension Schemes (Disclosure of Information) Regulations 2013.
 Police Act 1997 (Criminal Records) Regulations 2002.
 Pregnant Workers Directive (92/85/EEC).
 Protection of Children Act 1999.
 Protection of Freedoms Act 2012.
 Protection from Harassment Act 1997.
 Public Interest Disclosure Act 1998.
 Public Interest Disclosure (Compensation) Regulations 1999 (SI 1999/1548).
 Public Interest Disclosure (Prescribed Persons) Order 2014 (SI 2014/2418).
 Prescribed Persons (Reports on Disclosures of Information) Regulations 2017.
 Race Relations Act 1976.
 Redundancy Payments (Continuity of Employment in Local Government etc) (Modification) Order 1999.
 Regulation of Investigatory Powers Act 2000.
 Rehabilitation of Offenders Act 1974.
 Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975.
 Reserve Forces (Safeguard of Employment) Act 1985.
 Right to Time Off for Study or Training Regulations 2001.
 Safeguarding Vulnerable Groups Act 2006.
 Sex Discrimination Act 1975.
 Sex Discrimination Act 1975 (Amendment) Regulations 2008.
 Sex Discrimination (Gender Reassignment) Regulations 1999.
 Sex Discrimination (Indirect Discrimination and Burden of Proof) Regulations 2001.
 Shared Parental Leave Regulations 2014.
 Statutory Shared Parental Pay (Administration) Regulations 2014.
 Statutory Shared Parental Pay (General) Regulations 2014.
 Shared Parental Leave and Paternity and Adoption Leave (Adoption from Overseas) Regulations 2014.
 Statutory Shared Parental Pay (Parental Order Cases) Regulations 2014.
 Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.
 Temporary Agency Work Directive 2008.
 Trade Union Act 2016.
 Trade Union and Labour Relations (Consolidation) Act 1992.
 Transfer of Employment (Pension Protection) Regulations 2005.
 Transfer of Undertaking (Protection of Employment) Regulations 1981.
 Unfair Contract Terms Act 1997.
 Work and Families Act 2006.
 Working Time Regulations 1998 and 1999.
 Working Time (Amendment) Regulations 2002 and 2003.

'I know that there is nothing better for people than to be happy and to do good while they live.' Ecclesiastes 3:12

Directive on Written Information 91/533/EC.
Employment of Women, Young Persons and Children Act 1920.
Young Workers' Directive (Council Directive 94/33/EC).

Payroll

Approved Mileage Allowance Payments (Rates) Regulations 2011.
Attachment of Earnings Act 1971.
Automatic Enrolment (Earnings Trigger and Qualifying Earnings Band) Order 2014 and 2017.
Child Maintenance and Other Payments Act 2008.
Child Support Act 1991.
Child Support (Collection and Enforcement) Regulations 1992.
Civil Procedure Rules.
Commissioners for Revenue and Customs Act 2005.
Council Tax (Administration and Enforcement) Regulations 1992.
Courts Act 2003.
Education (Student Loans) (Repayment) Regulations 2000.
Employers' Duties (Implementation) Regulations 2010 (Auto enrolment).
Employers' Duties (Registration and Compliance) Regulations 2010.
Employment and Support Allowance Regulations 2008.
Income Tax (Earnings and Pensions) Act 2003.
Income Tax (Pay As You Earn) Regulations 2003.
Income Tax (Pay as you Earn) (Amendment) Regulations 2007.
Income Tax (Qualifying Child Care) Regulations 2007 and 2008.
National Insurance Contributions Act 2008, 2011 and 2014.
Occupational and Personal Pension Schemes (Automatic Enrolment) Regulations 2010.
Pensions Act 2008, 2011.
Social Security Act 1989.
Social Security Administration Act 1992.
Social Security Contributions & Benefits Act 1992.
Social Security Contributions Regulations 2001.
Social Security (Incapacity for Work) Act 1994.
Social Security (Overpayments and Recovery) Regulations 2013.
Statutory Maternity Pay and Statutory Adoption Pay (Curtailment) Regulations 2014.
Maternity Allowance (Curtailment) Regulations 2014.
Statutory Maternity Pay (General) Regulations 1986.
Statutory Maternity Pay (Medical Evidence) Regulations 1987.
Statutory Paternity Pay and Statutory Adoption Pay (General) Regulations 2002.
Statutory Paternity Pay and Statutory Adoption Pay (Weekly Rates) Regulations 2002.
Statutory Paternity Pay and Statutory Adoption Pay (Administration) Regulations 2002.
Statutory Paternity Pay (Adoption) and Statutory Adoption Pay (Adoptions from Overseas) (No.2) Regulations 2003.
Statutory Paternity Pay and Statutory Adoption Pay (Parental Orders and Prospective Adopters) Regulations 2014.
Statutory Sick Pay (General) Regulations 1982.

For the Local Government Pension Scheme:

The Local Government (Discretionary Payments) Regulations 1996.
The Local Government (Early termination) (Discretionary Compensation) (England and Wales) Regulations 2006.
The Local Government Pension Scheme (Amendment) Regulations 2015.
The Local Government Pension Scheme (Miscellaneous Amendments) Regulations 2014.
The Local Government Pension Scheme (Transitional Provisions, Savings and Amendment) Regulations 2014.
The Local Government Pension Scheme Regulations 2013 (as amended).
The Local Government and other Officers' Superannuation Act 1922.
The Local Government Superannuation Act 1937.
The Local Government Superannuation Act 1953.
The Local Government Superannuation Regulations 1974.

'I know that there is nothing better for people than to be happy and to do good while they live.' Ecclesiastes 3:12

The Local Government Superannuation Regulations 1986.
The Local Government Pension Scheme Regulations 1995.
The Local Government Pension Scheme Regulations 1997.
The Local Government Pension Scheme Transitional Provisions Regulations 1997 (as amended).
The Local Government Pension Scheme (Benefits, Membership and Contributions) Regulations 2007.
The Local Government Pension Scheme (Administration) Regulations 2008.
The Local Government Pension Scheme (Transitional Provisions) Regulations 2008.

For the NHS Pension Scheme:

NHS Pension Scheme Regulations 1995 and 2015.
NHS Pension Scheme Amendment Regulations, 2011, 2012, 2013, 2014, 2015, 2016 and 2017.

For the Teachers' Pension Scheme:

Teachers' Pension Regulations 2010 and 2014.
Teachers' Pension Regulations (Miscellaneous Amendments) 2011.
Teachers' Pension Regulations (Amendments) 2012, 2013, 2014.
Teachers' Pension Regulations (Amendments) (no 2) 2012.

Health and Safety

Health & Safety at Work Act 1974.
Management of Health and Safety at Work Regulations 1999.
Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013.
Safety Representatives and Safety Committees Regulations 1977.
Workplace (Health, Safety and Welfare) Regulations 1992.
Control of Substances Hazardous to Health Regulations 1999.
Health and Safety Information for Employees Regulations 1989.
Health and Safety (First Aid at Work) Regulations 1981.