The Chantry School
Data Protection Policy

Approved by:	Peter Jackson	**Date:**	24th May 2018
Last reviewed on:	24th May 2018		
Next review due by:	24th May 2019		

Contents

.....

1. 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.

2. Legislation and 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.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

3. 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 • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or 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.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

The 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.

5. Roles and 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.

5.1 Governing Board

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

5.2 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.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

Full details of the DPO's responsibilities are set out in their job description in appendix 1.

Our DPO is Peter Jackson, Acting Chair of Governors and is contactable by email at DPO@chantry.worcs.sch.uk

5.3 Data Protection Team

As well as the DPO, the school has implemented a team of staff in key roles to oversee data protection policy in school and to provide the DPO with information and support as required. The team consists of:

Andy Dickenson, Headteacher, who acts as the representative of the Data Controller on a day-to-day basis.

Dave Darling, Business Manager, who has been named as Chief Privacy Officer and will lead any internal administration on Data Protection.

Lorna Webster, Data Manager

Mark Carwardine, Network Manager

Lesley Webb, Lead Receptionist

A job team job description is set out in appendix 1.

All team members can be contacted by email at DPO@chantry.worcs.sch.uk

Please note that a collective email address is used for all those working in the team so that that there is transparency regarding any data requests or issues arising and that no one individual can make decisions or have opportunity to cover up any potential data protection issues.

5.4 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
- Contacting the DP team 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 there is a Subject Access Request directed to them
    - 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

6. Data Protection Principles

The GDPR is based on data protection principles that the 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.

7. Collecting Personal Data

7.1 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/carer when appropriate) 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 where the pupil is under 13 (except for online counselling and preventive services).

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

7.2 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 school's record retention schedule, which is based on version 5 of the Information and Records Management Society (IRMS) toolkit for schools.

8. 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/carer 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
- Government educational agencies e.g. ESFA, in order that we meet our statutory educational responsibilities

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.

9. Subject Access Requests and Other Rights of Individuals

9.1 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
- 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 or email to the DP team. 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 DP team unless it the request is considered to be a low level request as detailed in section 10.

9.2 Children and Subject Access Requests

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

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not 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. Refer also to section 10.

9.3 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 ask for written consent from any pupil aged 12 and over if the request is made by a parent or carer for the pupil's data, as per 9.2 above.
- 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.

9.4 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 DP team. If staff receive such a request, they must immediately forward it to the DP team.

10. Parental and Pupil Requests to see the Educational Record

The school will provide these free of charge and this will be treated by school staff in two different ways:

- A low level subject access request. This is for general information about a pupil's progress, expected grades, attendance, behaviour or personal contact / medical details stored in SIMS. This would be outside the normal school reporting timeframes. This information can be provided by any member of staff upon request by the parent or pupil verbally or in writing. This is because this information is normally presented to the parents and pupils at set times in the year. Low level requests will not be recorded.

- A normal subject access request. Parents or pupils may request more complex information due to issues that have arisen or are emerging and they believe there is information in the school domain not normally offered to them. This type of request will follow the normal subject access request process and will be dealt with by the DP team. These requests will be recorded.

11. Biometric Recognition Systems

Where we use pupils' biometric data as part of an automated biometric recognition system i.e. pupils use finger prints to receive school catering instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified of our biometric recognition system before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system. We provide an alternative means of accessing the relevant services for those pupils. Pupils are given a pin number to access catering services.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system, we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. The School also has a separate CCTV policy that is available on request.

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

Any enquiries about the CCTV system should be directed to the Business Manager.

13. Photographs and videos

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

We will obtain written consent from parents/carers for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

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

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

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

See our Digital Images Policy for more information on our use of photographs and videos.

14. Data Protection by Design and 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 / DP Team 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. A member of the DP team will carry out the PIA and will adopt the ICO code of practice when conducting a PIA https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
- Integrating data protection into internal documents including this policy, any related policies and privacy notices. Privacy Notices are attached in appendix 2.
- 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. A full Data Audit was carried out in April 2018.
- 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/DP team and all information we are required to share about how we use and process their personal data (via the privacy notice)
    - 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 and 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 and pupils are reminded to change their passwords at regular intervals

- Passwords are used to protect all portable devices and removable media, such as laptops and USB devices
- Secure email addresses will be provided where necessary e.g. Governors
- 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 the Acceptable Use Agreement.
- 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)
- The back up system is robust and managed in accordance with data protection principles. The back up process is attached in appendix 3.

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. The retention of different types of data is based on the IRMS Toolkit for schools and this document also shows how we dispose of each type of data.

Some key examples include:

We will shred or use a confidential waste bags for paper-based records e.g. printed payroll reports, Governors reports or pupil records.

We will destroy computer hard drives when computers become obsolete and overwrite or delete electronic files on laptops that are reallocated to other staff.

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 endeavors 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 below.

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

17.1 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/DP Team
- The DPO will investigate the report, and determine whether a breach has occurred with advice from the DP Team. 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 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
    - 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 on a password protected electronic file called 'Data Protection Confidential'. Only the DP team will have access to this file.
- 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:
    - 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 on a password protected electronic file called 'Data Protection Confidential'. Only the DP team will have access to this file.

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

17.2 Actions to Minimise the Impact of Data Breaches

We will take actions 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. Each breach and actions taken will be logged on a password protected electronic file called 'Data Protection Confidential'. Only the DP team will have access to this file.

An example of actions would include:

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 DP Team as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DP Team will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DP team 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 DP Team will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DP Team 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

18. Training

All staff and governors are provided with data protection training as part of their induction process.

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

The DPO is responsible for monitoring and reviewing this policy.

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). The Full Governing Body will authorise the policy following a recommendation by the DPO. It will then be reviewed after one year of operation to ensure it is working effectively. From then on, this policy will be reviewed **every 2 years** and shared with the Full Governing Board.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- CCTV Policy
- Digital Images Policy
- Acceptable Use Agreements
- Safeguarding Policy

21. Complaints Procedure

If you are unhappy with any aspect of the school's data protection processes or feel that you or your data hasn't been dealt with in accordance of the principles of this policy and the data protection regulations you can make a formal complaint. You should in the first instance write to:

Data Protection Officer
The Chantry School
Martley
Worcester
WR6 6QA

You should mark the letter as 'private and confidential'. The DPO will investigate the complaint and will respond within 30 days of receiving the written complaint.

If you are unhappy with the school response you can contact the Information Commissioner's Office at https://ico.org.uk and they will investigate your complaint with the school.

Appendix 1

The Chantry School

Role Description: Data Protection Officer (DPO)

General information

Contract type: Voluntary (Acting Chair of Governors)

Reporting to: Governing Body

Responsible for: Data Protection Team (DP Team)

Purpose

The DPO is responsible for monitoring compliance with current data protection law, and has the knowledge, support and authority to do so effectively. They oversee the school's data protection processes with day to day support from the DT Team and will advise the school on best practice.

Key responsibilities

To:

- Advise the school and its employees about their obligations under current data protection law, including the General Data Protection Regulation (GDPR)
- Develop an in-depth understanding of the school's processing operations, information systems, data security processes and needs, and administrative rules and procedures
- Monitor the school's compliance with data protection law, by ensuring the DP Team:
    - collect information to identify data processing activities
    - analyse and check the compliance of data processing activities
    - inform, advise and issue recommendations to the school and Governing Body
    - remain expert in data protection issues and changes to the law, attending relevant training as appropriate
- Ensure the school's policies are followed, through:
    - Assigning responsibilities to individuals in the DP Team
    - Awareness-raising activities through the DP Team
    - Co-ordinating staff training through the DT Team
    - Conducting internal data protection audits with the DP Team
- Advise on and assist the school with carrying out data protection impact assessments, if necessary
- Take decisions on data breach reporting after liaising with the DP Team.
- Act as a lead contact point for the Information Commissioner's Office (ICO), assisting and consulting it where necessary, including:
    - Helping the ICO to access documents and information
    - Seeking advice on data protection issues
- Act as a lead contact point for individuals whose data is processed (for example, staff, pupils and parents), including:
    - Responding to subject access requests as appropriate
    - Responding to other requests regarding individuals' rights over their data and how it is used
- Take a risk-based approach to data protection, including:
    - Prioritising the higher-risk areas of data protection and focusing mostly on these
    - Advising the school if/when it should conduct an audit, which areas staff need training in, and what the DPO role should involve
- Report to the Governing body on the school's data protection compliance and associated risks

- Respect and uphold confidentiality, as appropriate and in line with data protection law, in carrying out all duties of the role
- Undertake any additional tasks necessary to keep the school compliant with data protection law and be successful in the role
- Ensure the DP team maintain a record of the school's data processing activities
- Ensure the DP Team work with external stakeholders, such as suppliers or members of the community, on data protection issues
- Take responsibility with the DP team for fostering a culture of data protection throughout the school
- Ensure the DP Team work closely with other departments and services to ensure GDPR compliance, such as HR, legal, IT and security.

The Role of the DP Team

The team consists of:

The Headteacher, as Head of School and ICO contact

The Business Manager, who will act as Chief Privacy Officer with a lead day to day role in Data Protection

Data and SIMS Manager, as the key Data Processor of software in school

Network Manager, as the key provider of data processing devices in school

Lead Receptionist, as a key staff member in Data Processing and an immediate contact for parents and pupils.

All members of the team will support the DPO in carrying out their role by ensuring that:

- day to day data protection processes are carried out according to the law and that there is ongoing audit and monitoring of these practices to ensure compliance
- that induction and training is delivered to all staff and that there is a culture of data protection in place
- Subject access requests are handled appropriately
- Potential data breaches are dealt with quickly and appropriately
- External suppliers and stakeholders are compliant with the law

DPO - Person specification

Criteria	Desirable qualities
Qualifications	• Background in law, information security, data protection or IT desired • Educated to degree level, or equivalent professional experience • Relevant data protection training desired
Experience	• Professional experience of data protection law • Experience of managing data protection compliance
Skills and knowledge	• Knowledge of data protection law (the GDPR and Data Protection Act 1998) • Knowledge of information security and data processing principles and good practice • An understanding of school software systems e.g. SIMS • Excellent communication skills • Excellent teamwork and interpersonal skills, with proven ability to maintain relationships across a school or other organisations • Ability to explain complex data protection and information security information to a non-specialist audience
Personal qualities	• Detail-oriented • Ability to work under pressure • Ability to prioritise tasks effectively • Ability to work independently and autonomously with minimal supervision • Commitment to maintaining confidentiality at all times

PRIVACY NOTICE
for
THE CHANTRY SCHOOL

Privacy Notice - How we use pupil information

Why we collect and use this information

We **The Chantry School** are the 'data controller' for the purposes of data protection law.
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:

- 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
- to safeguard students
- Support a Young Person in their transition to a Post-16 Provider of Education or Training.

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

- Personal information (such as name, unique pupil number and contact details)
- 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 and Disability
- Behaviour and exclusions
- Education/school history
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school

Collecting pupil information

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

Storing pupil information

Personal data relating to pupils at The Chantry School and their families, is stored in line with the school's GDPR Data Protection Policy, which can be viewed on our school website.

Who we share pupil information with

We routinely share pupil information with:

- schools that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)

In accordance with Data Protection Law, The Chantry School enlists the support of companies to act as data processors. This information is processed on our behalf to enable us to support your needs more effectively. These companies enable us to provide services to our pupils, parents and staff to support the efficient functioning of the school. Such companies include, Capita (SIMS), Sisra, Nationwide (Cashless catering system) and Schoolcomms. This list is not an exhaustive list of all data processors used by The Chantry School. Decisions on whether to release this data are subject to a robust approval process and contractual assurances that personal data will be kept securely and only in accordance with the school's specific directions.

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 are required by law to provide information about pupils to the Department for Education as part of statutory data collections such as the school census. This data sharing underpins school funding and educational attainment policy and monitoring. We are required by law to share information about our pupils with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

The National Pupil Database (NPD)

Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.

For more information, see the Department's webpage on how it collects and shares research data.

For more information on how this sharing process works, please visit:

https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract

For information on which third party organisations (and for which project) pupil level data has been provided to, please visit: https://www.gov.uk/government/publications/national-pupil-database-requests-received

If you need more information about how our local authority collect and use your information, please visit:
Our local authority at http://www.worcestershire.gov.uk/ and search for privacy notice.

Youth support services

Once our pupils reach the age of 13, the law requires us to pass on certain information to our local authority and/or the youth support services provider as they have legal responsibilities in relation to the education or training of 13-19 year olds.

This information enables them to provide youth support services, post-16 education and training services, and careers advisers.

We provide them with these pupils' names and addresses, dates of birth, name(s)/address(es) of their parent(s)/carer and any other information relevant to their role. We may also share certain personal data relating to children aged 16 and over with post-16 education and training providers in order to secure appropriate services for them

However, a parent/carer can ask that no information beyond names, addresses and date of birth be passed to the youth support service by informing **Mrs L Webster.** This right is transferred to the child once he/she reaches age 16. For more information about services for young people, please go to our local authority website http://www.worcestershire.gov.uk/.

For more information about young people's services, please go to the National Careers Service page at https://nationalcareersservice.direct.gov.uk/aboutus/Pages/default.aspx

Parents and pupils' rights regarding personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold.

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

Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

If you would like to make a request please contact our data protection officer, Mr Peter Jackson by emailing dpo@chantry.worcs.sch.uk

Appendix 2b

PRIVACY NOTICE

for

THE CHANTRY SCHOOL

Privacy Notice – How we use school workforce information

The Chantry School collects, uses and is responsible for certain personal information about you. When we do so we are regulated under the General Data Protection Regulation which applies across the European Union (including in the United Kingdom) and we are responsible as 'controller' of that personal information for the purposes of those laws. Our Data Protection Officer is **Mr Peter Jackson.**

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)
- relevant medical information

Why we collect and use this information

We use school workforce data to:

- Enable individuals to be paid
- Support pension payments and calculations
- Enable sickness monitoring
- Enable leave payments (such as sick pay and maternity leave)
- Develop a comprehensive picture of the workforce and how it is deployed
- Inform the development of recruitment and retention policies
- Inform financial audits of the school
- Fulfil our duty of care towards our staff

The lawful basis on which we process this information

We collect and use staff information under the Education Act 1996. The EU general data protection regulation 2016/679 (GDPR) will take effect in May 25 2018 including Article 6 'lawfulness of processing' and Article 9 'Processing of special categories of personal data'.

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 no longer than is necessary. We follow the recommended retention period specified in the Information Records Management Society – Retention Guidelines for Schools document which can be found at www.irms.org.uk

Who we share this information with

We routinely share this information with:

- our HR and Payroll provider
- 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.

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

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

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 dpo@chantry.worcs.sch.uk

You also have the right to:

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

If you have a concern about the way we are collecting or using your personal data, 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: dpo@chantry.worcs.sch.uk

Appendix 3

The Chantry School Server Backup Schedule

Backup Exec – Server01 System State, C, D and H Full Every Night at 8pm to rotating 5 day RDX tapes (kept in fire safe in our office)

Windows Backup: System States, C, D + H Drives

Source	Time Run	Includes	Destination	Typical Duration
Server02	22:00 Daily	SYS State, Bare Metal,C, D and H	Local USB External Disk	1 Hour
Server03	01:30 Daily	SYS State, Bare Metal,C, D and H	Local USB External Disk	45 Mins

Macrium Reflect

Source	Time Run	Includes	Destination	Typical Duration
Exchange	22:00	Full Image	Nasbox2 Daily + Weekly to Quad Station	4.5 Hours
Dcchanthadmin	02:30	Full Image	Nasbox2 Daily + Weekly to Quad Station	5 Hours
Membersrv1	11:30 Sat Weekly	OS Image	Nasbox2	30 Mins
Membersrv2	10:30 Sat Weekly	OS Image	Nasbox2	30 Mins
Server01	06:00 Sun Weekly Plus Weekday Differentials	Full Image	Nasbox2	
Server02	12:00 Sat Weekly	OS Image	Nasbox2	
Server03	16:00 Sat Weekly	OS Image	Nasbox2	

Backup Assist: Exchange Mailbox Backup

Email Mailbox backup each night at 5pm to Quad Station (4.5 Hours)

SyncBackupPro:

Cumulative Backups (for end user file recovery): -

Source	Time Run	Includes	Destination	Typical Duration

Server01	06:00	H Drive (users and staff shared)	Nasbox1	1 Hours
Server02	17:00	H Drive (users)	Nasbox1	2 Hours
Server03	21:00	H Drive (users)	Nasbox1	1 Hour
Dcchanthadmin	12:00	D Drive (users, sims, finance)	Nasbox1	1 Hour
Membersrv1	02:00	Music Shared + Pupil Resources	Nasbox1	Less than 30 mins
Membersrv2	01:15+ 23:30	Media Shared + Pupil Shared	Nasbox1	Less than 30 mins

Mirror Backups (for data recovery): -

Source	Time Run	Includes	Destination	Typical Duration
Dcchanthadmin	01:00	D Drive	Nasbox1	1 Hour
Server02	Weekly-Sat 09:00	D Drive	Nasbox1	-
Server03	Weekly-Sun 09:30	D Drive	Nasbox1	-
Server02	19:00	H Drive	Nasbox1	1.5 Hours
Server03	22:15	H Drive	Nasbox1	45 mins

Additional Extra Backups of key data: -

Source	Includes	Destination
Dcchanthadmin	Finance system	Membersrv2
Dcchanthadmin	SIMS	Membersrv2
Dcchanthadmin	School Fund	Membersrv2
Dcchanthadmin	Weekly SIMS	Membersrv2
Server01	Staff Shared	Membersrv2
Room Booking Virtual PC	Room Booking DB's	Nasbox1
Cashless Catering PC	Cashless Catering DB	Nasbox1

Useful Information

- Macrium Reflect Recovery CD's are kept in the firesafe and also the image files of these CD's are saved in:

- *nasbox1\media\Macrium Reflect Rescue CDs*.

- The Backup Exec Disaster Recovery File (alternate saved location) is in:

  \\nasbox1\BACKUPS\Server01\Disaster Recovery Data For BackupExec

- Nasbox1 and Nasbox2 are kept in our office. The Quad Station is in the server room attached to the Exchange Server.

- The cumulative backups need to be archived once a year to stop them getting too large and affecting the backup times.

- RM prefer us to use Backup Exec for Server01 and to use windows backup for the additional curriculum servers.

- IBS prefer us to use Macrium Reflect.