GDPR (Data Protection) Policy

Date approved: 20.03.19
Signed by Chair of Governors: Mr Paul Rossi

Date approved: 20.03.19
Signed by Headteacher: Mr Sean Hayes

Reviewed:
Next Review: 20.03.20

St John Fisher
Catholic High School

Policy and Procedures

Contents

GDPR POLICY

General Data Protection Regulation

St John Fisher Catholic High School is the data controller for the purposes of the Data Protection Act and General Data Protection Regulations.

We are committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the General Data Protection Act that became enforceable in May 2018.

https://ico.org.uk/for-organisations/guide-to-data-protection/data-protectionprinciples/

Changes to data protection legislation (GDPR May 2018) shall be monitored and implemented in order to remain compliant with all requirements.

The legal bases for processing data:

Student Data

A school is considered to be a public body and it is considered to be in the public interest that we operate schools and educate children. Accordingly, for all the common tasks carried out by schools we do not need to ask for the data subject's consent but rather we can use 'public interest' as our legal basis for processing the appropriate personal data including special categories of personal data.

Staff, Parents and Governors

We process this information under the Data Protection Act 1998, and according to guidance published by the Information Commissioner's Office and the Department for Education. Under Article 6 of the GDPR, effective 25 May 2018, the lawful basis for processing school workforce, parents and governors information is to fulfil legal, contractual obligations and other legitimate interests. For data collection purposes (Departmental Censuses) provisions of the Education Act 1996 will be followed. Consent will be requested for specific activities (at the time of activity) where activities require processing of data if deemed suitable.

The school is committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided.

The GDPR requirements stated in policy and other supporting documents and processes are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

These documents include but are not limited to:

- Student Privacy Notice
- Staff Privacy Notice
- ICT Security Policy
- ICT Acceptable Use Policy
- Supplier Data Processing Agreement
- Data Erasure & Consent withdrawal request

Registration with the ICO

Our data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO.

A Data Protection Officer (DPO) has been appointed to help the school fulfil its responsibilities relating to the GDPR.

Personal and Sensitive Data:

All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/keydefinitions/

The principles of the Data Protection Act shall be applied to all data processed:

- Processed fairly, lawfully and in a transparent manner
- Used for specified, explicit and legitimate purposes
- Used in a way that is adequate, relevant and limited
- Accurate and kept up-to-date
- Kept no longer than is necessary
- Processed in a manner that ensures appropriate security of the data

Fair Processing / Privacy Notice:

We shall be transparent about the intended processing of data and communicate these intentions via notification to governors, staff, parents and pupils prior to the processing of individual's data.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation. https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-noticestransparency-and-control/

There may be circumstances where the school is required to pass information onto external parties.

For our Staff, Contractors or Governors, these include:

- Our local authority
- Statutory & Regulatory Bodies e.g. HMRC, Department for Work and Pensions
- Regulatory Bodies e.g. Ofsted
- The Department for Education (DfE)

- Approved suppliers providing essential services to the school. This information is only shared to ensure the performance of their contracted duties. These suppliers are bound to the GDPR responsibilities by contract and law.

For our Parents and Pupils these include:

- schools that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)
- School Nurse
- NHS
- Other organisations which assist with assessment and evaluation of students' progress.

There may be unavoidable disclosures, for example, to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form undertaking not to disclose the data outside the school. Officers and IT personnel writing on behalf of the LEA are IT liaison/data processing officers, for example in the LEA, are contractually bound not to disclose personal data.

Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who **needs to know** the information in order to do their work. The school will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything which suggests that they are, or have been, either the subject of or at risk of child abuse.

A **"legal disclosure"** is the release of personal information from the computer to someone who requires the information to do his or her job within or for the school, provided that the purpose of that information has been registered.

An **"illegal disclosure"** is the release of information to someone who does not need it, or has no right to it, or one which falls outside the School's / Centre's registered purposes. It is worth noting that comments on social media which disclose privileged personal data would fall into the category of "illegal disclosure".

For more information about the DFE 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

Consent

Consent will be sought prior to processing any data which cannot be done so under any other lawful basis, such as complying with a regulatory requirement. Where consent is given, a record will be kept documenting how and when consent was given. Consent can be withdrawn by the individual at any time.

How consent affects staff and pupils respectively is detailed in the Staff and Pupil Privacy Notices.

Photographs, Video and CCTV:

The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only.

Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources.

It is the school's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent.

The school notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.
Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose. All CCTV footage will be kept for 10 days for security purposes.

The right to be informed:

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The contact details of the controller (the school), and the controller's contact person
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data
- Details of transfers to third countries and the safeguards in place.
- The retention period and criteria used to determine the retention period.
- The existence of the data subject's rights

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied within one month of having obtained the data.

The right of access - Subject Access Requests:

Under data protection legislation, school staff, governors, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, the Subject Access Request for should be completed and emailed to the Senior Administrator on SubjectAccessRequest@stjohnfisherschool.org.uk.

The request will be completed within one calendar month and there will be no charge to fulfil the request.

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

In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information that is required.

The right to rectification:

School staff, governors, parents and pupils have the right to request any inaccurate or incomplete personal data be rectified. Where the data in question has been disclosed to anyone else, the school will inform them of the rectification. If relevant, the school will inform the individual of whom the data has been disclosed to.

The request for rectification will be completed within one month.

Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority.

Data Erasure & Consent withdrawal request

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for the data to be retained.

An example of such a circumstance could be:

- When the individual withdraws their consent
- Where the personal data is no longer necessary for the purpose it was recorded originally
- When the individual objects to the use of their data and there is no overriding legitimate reason to continue the use of the data
- The processing of the data was unlawful
- There is a legal reason to erase the data

The school has the right to refuse the request of erasure for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

The right to restrict processing

Individuals have the right to block or suppress the school's processing of personal data.
In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future

The school will restrict the processing of data under the following circumstances:

- The individual contests the accuracy of their data
- The individual has objected to their data being used and the school is considering if there are legitimate ground to override the request
- Where the processing of someone's data is seen as unlawful and they request restriction
- In the event that the data is no longer needed by the school, but the individual requires the data to exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The school will inform individuals when a restriction on processing has been lifted.

The right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner.

The right to data portability only applies in the following cases:

- To personal data that the individual provided to the school
- Where the data is being processed based on someone's consent for the performance of the contract
- When data processing is carried out by automated method

The school will provide the information free of charge. The data will be provided in standard computer format or directly sent to another organisation at the request of the individual.
Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to object

The school will inform individuals of their right to object and this information will be outlined in the privacy notice.

Individuals have the right to object to the following:

- The data being processed for legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics

Where personal data is processed for the performance of a legal task or legitimate interest, the objection must be specifically related to their situation.

The school will stop processing the individual's personal data unless the processing is required for a legal defence or the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual affected.

If their data is being used for marketing related purposes.

The school is not required to comply with an objection if the data processing is required for the performance of a public interest task.

If the data processing activities above are performed online, then a method to object will be available.

Privacy by design and privacy impact assessments

The school will adopt a privacy by design approach and implement the required technical and organisational measures to integrate data protection as part of the daily operation.

The goal is to:

- Minimise personal data processing
- Only process data that is necessary and to the extent that is necessary
- Retain data only for as long is necessary

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations

DPIAs will allow the school to identify and resolve problems at an early stage.
A DPIA will be carried out when using new technologies or when the processing of data poses high risk.

High risk processing includes:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV

The school will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where a DPIA has indicated high risk data processing, the school will consult the ICO to ensure that the processing activity conform to the GDPR.

Data Breach

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.

The School will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their staff training.

Data retention

Data will not be kept for longer than is necessary. Unrequired data will be deleted as soon as practicable.

Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

Disposal of IT assets holding data shall be in compliance with ICO guidance:
https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf

Data and IT Security:

St John Fisher Catholic High School undertakes to ensure security of personal data in the following ways:

Physical Security

Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the computer room. Disks, tapes and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.

IT Security

The internal computer network and devices are protected by an industry recognised Firewall which has been professionally installed and maintained. All external access such as remote working and internet access is monitored and managed by the internal IT Support Team and the schools external IT Support Partner.

Anti-Virus Software and Safeguarding Software is installed on all computers containing personal data. Only authorised users are allowed access to the data and password changes are regularly undertaken. All data is backed up regularly. Clearly, many documents in school contain sensitive and personal data. (For example, IEPs, SEN statements and annual reviews, exclusion letters). A screen lock policy, locks any computer screen if there is an inactivity of more than 15 minutes, ensuring that a computer is not left unattended and open for unauthorised access.

Great care must be taken when any data is taken off-site. USB Storage devices such as memory sticks are no longer permitted for general use. These devices are now only permitted for temporary essential use and for specialist tasks such as Dictaphones or Cameras. In the event that a specific task requires such a device, an encrypted, authorised device is available from the I.T. Services Department for temporary use.

The use of laptops has been minimised, reducing the risk of school data being lost or stolen. The remaining laptops have been encrypted to avoid unauthorised access.

An IT Acceptable Use Policy and IT Security Policy governs the use of IT Systems within the school and technical assistance with this is available from the IT Services Department in school.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:

https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/02/privacyimpact-assessments-code-published/

Security of data shall be achieved through the implementation of I.T Security Systems and Internal Processes.

The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data and their implementation of the GDPR guidelines.

DBS data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

Data provided by the DBS will never be duplicated.

Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

This policy is reviewed every two years. The next scheduled review date for this policy is July 2020.

Further information

If you have a concern about the way we are collecting or using your personal data, or wish to discuss anything in this policy we ask that you raise your concern with the HR department on HR@stjohnfisherschool.org.uk in the first instance.

Alternatively, you can contact the School's Data Protection Officer via email: DPO@stjohnfisherschool.org.uk

You can also contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Reviewed by the Finance and Premises Meeting: March 2019

Next Review Date: March 2020 **Staff Member Responsible:** SBM