ST. HELEN'S CATHOLIC PRIMARY SCHOOL

Mission statement

Respect yourself
Respect everyone in our school community,
Respect everyone in our local community,
Respect everyone in our global community,
But most of all, respect God our father in Heaven.

General Data Protection Regulation Policy

Our Commitment:
The Governors of St Helen's Catholic Primary School 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 Regulation (GDPR).

Changes to data protection legislation (GDPR May 2018) will be monitored and implemented in order to remain compliant with all requirements.
The member of staff responsible for data protection is Mrs Curtis. However all staff must treat all pupil /staff/parent information in a confidential manner and follow the guidelines as set out in this document.
The school is also committed to ensuring that our staff are aware of data protection policies, legal requirements and adequate training is provided to them.
The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive personal data	Data such as: • Contact details • Date of Birth • Telephone number etc.
Special category data	• race; • ethnic origin; • politics; • religion; • trade union membership; • genetics; • biometrics (where used for ID purposes); • health; • sexual orientation.

Criminal offence data	The GDPR rules for sensitive (special category) data do not apply to information about criminal allegations, proceedings or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures.
Processing	Obtaining, recording or holding data
Data subject	The person whose personal data is held or processed
Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed (school)
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

The GDPR sets out **six** data protection principles as follows;

Principle 1.

Data must be processed lawfully, fairly and in a transparent manner in relation to individuals;
Schools must have a **valid lawful basis** in order to process personal data
There are six available lawful bases for processing. No single basis is 'better' or more important than the others. Most lawful bases require that processing is 'necessary'.

a) Consent: the individual has given clear consent for the school to process their personal data for a specific purpose.

b) Contract: the processing is necessary for a contract the school has with the individual, or because they have asked the school to take specific steps before entering into a contract.

c) Legal obligation: the processing is necessary for the school to comply with the law (not including contractual obligations).

d) Vital interests: the processing is necessary to protect someone's life.

e) Public task: the processing is necessary if you are a public authority that needs to process the information to carry out your official functions.

f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Additional Lawful bases include:

Special category data

This is personal data which the GDPR says is more sensitive, and so needs more protection.
See table above
Schools must still have a lawful basis for processing special category data under **Article 6**, in exactly the same way as for any other personal data. The difference is that you will also need to satisfy a specific condition under **Article 9.**

Criminal offence data
To process personal data about criminal convictions or offences, you must have both a lawful basis under **Article 6** and either legal authority or official authority for the processing under **Article 10.**

Principle 2
Data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Principle 3
Processed data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
Principle 4
Processed data should be accurate and, where necessary, kept up to date.
Principle 5
Data should be kept in a form which permits identification of data subjects for *no longer than is necessary* for the purposes for which the personal data are processed.
Principle 6
Data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

There are two further underpinning principles. The first underpinning principle is:

1. The principle of Individual Rights

The GDPR provides the following rights for individuals:

a) The right to be informed (Fair Processing / Privacy Notice)

Being transparent and providing accessible information to individuals about how you will use their personal data is a key element of the Data Protection Act 1998 (DPA) and the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a privacy notice.

b) The right of access (Subject access requests)

Individuals have the right to access their personal data and supplementary information.
The right of access allows individuals to be aware of and verify the lawfulness of the processing. No charge will be applied to process the request.

c) The right to rectification

The GDPR gives individuals the right to have personal data rectified. Personal data can be rectified if it is inaccurate or incomplete.

d) The right to erasure

The right to erasure is also known as 'the right to be forgotten'.
The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
The right to erasure does not provide an absolute 'right to be forgotten'.

e) The right to restrict processing

- Individuals have a right to 'block' or suppress processing of personal data.
- When processing is restricted, you are permitted to store the personal data, but not further process it.
- You can retain just enough information about the individual to ensure that the restriction is respected in future

f) The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

g) The right to object

Individuals have the right to object to:

You must inform individuals of their right to object "at the point of first communication" and in your privacy notice.

h) Rights in relation to automated decision making and profiling.

The GDPR has provisions on:

- automated individual decision-making (making a decision solely by automated means without any human involvement);and
- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

The second underpinning principle is:

2. The principle of Accountability and governance.

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance.

a) Contracts

- Whenever a controller uses a processor it needs to have a written contract in place.
- The contract is important so that both parties understand their responsibilities and liabilities.
- The GDPR sets out what needs to be included in the contract.

a) Documentation

The documentation of processing activities is a new requirement under the GDPR.

The GDPR contains explicit provisions about documenting your processing activities.

- You must maintain records on several things such as processing purposes, data sharing and retention.

b) Data Protection by design and default

Under the GDPR, you have a general obligation to implement technical and organisational measures to show that you have considered and integrated data protection into your processing activities.

Privacy Impact Assessments (PIAs) are an integral part of taking privacy by design approach.

Privacy impact assessments (PIAs) are a tool that you can use to identify and reduce the privacy risks of your projects.

c) Data Protection impact Assessments

Data protection impact assessments (also known as privacy impact assessments or PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

d) Data protection officers

The GDPR makes it a requirement that organisations appoint a data protection officer (DPO) in *some* circumstances.

e) Codes of conduct and certification

The GDPR endorses the use of approved codes of conduct and certification mechanisms to demonstrate that you comply.

Signing up to a code of conduct or certification scheme is not obligatory. But if an approved code of conduct or certification scheme that covers your processing activity becomes available, you may wish to consider working towards it as a way of demonstrating that you comply.

Data protection Fee

The Government has announced a new charging structure for data controllers to ensure the continued funding of the Information Commissioner's Office (ICO).

The new structure was laid before Parliament as a Statutory Instrument and will come into effect on 25 May 2018, to coincide with the General Data Protection Regulation.

Until then, organisations are legally required to pay the current notification fee, unless they are exempt.

Data Security

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

International transfers

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations

Transfers may be made where the Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection

Personal data breaches

- The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.
- You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

In addition school staff must also take into account the following checklist

General Data Protection Regulation checklist

School staff

Regularly change your passwords (Recommended every 30 days)
Log off or lock your computer when away from your desk or use a screen saver when away from your computer
Dispose of confidential waste securely by shredding
Operate a clear desk system
Orange folders/SEN/EAL folders kept in locked cupboards. Pupil files must be locked away
Collect only the personal information you need for a particular purpose
Do not give out personal data or information about a child or member of staff over the phone without following up the call with an email to the recipient.

Do not title any email with any name of a child or adult.
Staff are not permitted to use pen drives or external hard drive to store information between home and school.
When using your school laptop at home to access the remote system please ensure you always log out.
All teaching staff must read and sign the Remote Access policy
All PC/Laptop screens positioned away from outside windows when accessing personal/school data and interactive whiteboards must be turned off. Freeze screen
Only use password protection when sending confidential emails using only the school's address
Ensure all email alerts are turned off when the screen is visible to others, including children.
Ensure that the Business Manager is aware of changes in your personal details as soon as possible
If you think you or someone else has breached the GDPR then you must tell the Headteacher as soon as possible.
Reminders about photos not going on social media at all parent/public events
Medical bags must not be left outside etc.
Reports need to be checked to make sure that both pages are for that child and in the correct envelope with the correct attendance etc.

School IT protection

Ensure the school is protected from virus attacked by taking care when opening emails and attachments from unknown sources.
Ensure the school keeps back-ups of information
Check outside providers are GDPR compliant
Schools has clear procedures for IT hardware to be confidentially destroyed
School has a clear Business Continuity Plan and Disaster Plan
All school laptops and Ipads are assigned to staff members and have been signed by the staff member to use and to be accountable if taken off site. If equipment is not taken off site then appropriately locked away when not in use.
Documents sent to the printer should always be collected and not left in the printer where sensitive information may be on display
All IT devices have suitable anti-malware and anti-virus software which is running and up to date. If in doubt write in James' book (IT technician) or see Mrs Watkins.
Only the Headteacher can erase or delete electronic records or give permission for information to be erased.

General school protection

Visitors sign in and out of premises and are advised of DBS, medical and fire procedures
Update records promptly e.g. change of address. SEN, Assessment, PP etc.
Be aware that people may try to trick you to give out personal information. All identify checks must be made first.
Read and sign the Records Management Policy
Read and sign the GDPR policy
Read the Privacy notice for staff and parents
If this is your role do know how to recognise a subject access request?
If this your role do know who to pass on a subject access request?
If this is your role do you know you have a calendar month to process the request?
If this is your role do you know that they may need to check the identity of the requester?
Do you know what to do to if other people's information is contained in the proposed response?
Are there procedures in place which allows individual to request the deletion or erasure of their information that the school holds where there is no compelling reason for its continued processing?
Review the school's privacy notices to ensure the school informs individuals of their right to object "at the point of first communication" and should be displayed clearly
Ensure parents are aware yearly that when consent has been given for photographs, trips etc. they can opt back out of that consent.

Ensure that when a child is no longer attending the school that consent has been given from parents to send the school's information to the next school, this includes Year 6 transition.
If any information is shared accidently with you from external agencies please inform them via email and return the information, as well as telling them they need to inform the ICO.

Children

- Children need particular protection when collecting and processing their personal data because they may be less aware of the risks involved.
- Compliance with the data protection principles and in particular fairness should be central to all processing of children's personal data.
- Clear privacy notices should be written for children so that they are able to understand what will happen to their personal data, and what rights they have.
- Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.
- An individual's right to erasure is particularly relevant if they gave their consent to processing when they were a child.

This policy will be reviewed yearly.