SACRED HEART HIGH SCHOOL

GDPR & DATA PROTECTION POLICY

JULY 2021

To be reviewed July 2022

Contents

		Page
1	**POLICY OBJECTIVES**	4
2	**SCOPE OF THE POLICY**	4
3	**THE PRINCIPLES**	4
4	**TRANSFER LIMITATION**	5
5	**LAWFUL BASIS FOR PROCESSING PERSONAL INFORMATION**	5
6	**SENSITIVE PERSONAL INFORMATION**	6
7	**AUTOMATED DECISION MAKING**	7
8	**DATA PROTECTION IMPACT ASSESSMENTS (DPIA)**	7
9	**DOCUMENTATION AND RECORDS**	8
10	**PRIVACY NOTICE**	9
11	**PURPOSE LIMITATION**	10
12	**DATA MINIMISATION**	10
13	**INDIVIDUAL RIGHTS**	10
14	**INFORMATION SECURITY**	11
15	**INDIVIDUAL RESPONSIBILITIES**	12
	15.1 General	12
	15.2 Sending emails	13
	15.3 In classrooms	13
	15.4 Remote Connection	13
	15.5 Screen Locking	13
	15.6 Replacement for Computer Sticks (USB keys)	13
	15.7 Storing Files	14
	15.8 Hard copies	14
16	**STORAGE AND RETENTION OF PERSONAL INFORMATION**	14
17	**DATA BREACHES**	14
	17.1 What is a Data Breach?	14
	17.2 Types of Data Breach	15
18	**DATA BREACH PROCEDURE**	15
	18.1 Determining if a Breach has Occurred	15
	18.2 Process if Breach is Confirmed	16
	18.3 Assessing the Need to Report to Information Commissioner	16
	18.4 Reporting to the Information Commissioner	17

18.5 Reporting to Individuals whose data has been breached 17
18.6 Reporting to Third Parties 17
18.7 Review 18
19 TRAINING 18
20 CONSEQUENCES OF A FAILURE TO COMPLY 18
21 THE SUPERVISORY AUTHORITY IN THE UK 18
22 REVIEW AND RATIFICATION 18
GLOSSARY 18

RATIONALE

General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

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

1 POLICY OBJECTIVES

The school as the Data Controller will comply with its obligations under the GDPR and DPA. The school is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation.

All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy.

The Information Commissioner as the Regulator can impose fines of up to 20 million Euros (approximately £17 million) for serious breaches of the GDPR, therefore it is imperative that the School and all staff comply with the legislation.

2 SCOPE OF THE POLICY

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information[1]. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the GDPR personal information also includes an identifier such as a name, an identification number, location data or an online identifier.

The School collects a large amount of personal data every year including: pupil records, staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the School. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

Biometric information is not currently held by the school at all. Specific provisions to protect such data would be agreed in a revised version of this policy to comply with statutory requirements before the introduction of any biometric system in the future.

3 THE PRINCIPLES

The principles set out in the GDPR must be adhered to when processing personal data:

1. Personal data must be processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**)

[1] GDPR Article 4 Definitions

2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**)
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (**data minimisation**)
4. Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (**accuracy**).
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed (**storage limitation**)
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information are processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (**integrity and confidentiality**).

4 TRANSFER LIMITATION

In addition, personal data shall not be transferred to a country outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data as determined by the European Commission or where the organisation receiving the data has provided adequate safeguards2.

This means that individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. It may also be possible to transfer data where the data subject has provided explicit consent or for other limited reasons. Staff should contact the DPO if they require further assistance with a proposed transfer of personal data outside of the EEA.

5 LAWFUL BASIS FOR PROCESSING PERSONAL INFORMATION

Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected:

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the school
- Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the data controller is subject

[2] These may be provided by a legally binding agreement between public authorities or bodies, standard data protection clauses provided by the ICO or certification under an approved mechanism.

- Processing is necessary in order to protect the vital interests of the data subject or of another natural person

- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party[3]

- The data subject has given consent to the processing of his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, the consent from be kept separate from those other matters

- Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first consented.

The decision as to which lawful basis applies must be documented, to demonstrate compliance with the data protection principles and include information about both the purposes of the processing and the lawful basis for it in the school's relevant privacy notice(s).

When determining whether legitimate interests are the most appropriate basis for lawful processing (only where appropriate outside the school's public tasks) a legitimate interests assessment must be carried out and recorded. Where a significant privacy impact is identified, a data protection impact assessment (DPIA) may also need to be conducted.

6 SENSITIVE PERSONAL INFORMATION

Processing of sensitive personal information (known as 'special categories of personal data') is prohibited[4] unless a lawful special condition for processing is identified.

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

- There is a lawful basis for doing so as identified on previous page

- One of the special conditions for processing sensitive personal information applies:

[3] The GDPR states that legitimate interests do not apply to processing carried out by public authorities in the performance of their tasks, Article 6 However, the ICO indicates that where there are other legitimate purposes outside the scope of the tasks as a public authority, legitimate interests may be considered where appropriate (particularly relevant for public authorities with commercial interests).

[4] GDPR, Article 9

(a) the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)
(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the school or the data subject
(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
(d) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim
(e) the processing relates to personal data which are manifestly made public by the data subject
(f) the processing is necessary for the establishment, exercise or defence of legal claims
(g) the processing is necessary for reasons of substantial public interest
(h) the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services
(i) the processing is necessary for reasons of public interest in the area of public health.

The school's privacy notice(s) set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Unless the School can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. Evidence of consent will need to be captured and recorded so that the school can demonstrate compliance with the GDPR.

7 AUTOMATED DECISION MAKING

Where the school carries out automated decision making (including profiling) it must meet all the principles and have a lawful basis for the processing. Explicit consent will usually be required for automated decision making (unless it is authorised by law or it is necessary for the performance of or entering into a contract).

Additional safeguards and restrictions apply in the case of solely automated decision-making, including profiling. The School must as soon as reasonably possible notify the data subject in writing that a decision has been taken based on solely automated processing and that the data subject may request the school to reconsider or take a new decision. If such a request is received staff must contact the DPO as the school must reply within 21 days.

8 DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

All data controllers are required to implement 'Privacy by Design' when processing personal data.

This means the School's processes must embed privacy considerations and incorporate appropriate technical and organisational measures (like pseudonymisation) in an effective manner to ensure compliance with data privacy principles.

Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a DPIA must be carried out to assess:

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals; and
- what measures can be put in place to address those risks and protect personal information.

Staff should adhere to the Data Protection Toolkit for Schools from the DfE with reference to the DPIA template.

When carrying out a DPIA, staff should seek the advice of the DPO for support and guidance and once complete, refer the finalised document to the DPO for sign off.

9 DOCUMENTATION AND RECORDS

Written records of processing activities must be kept and recorded including:

- the name(s) and details of individuals or roles that carry out the processing;
- the purposes of the processing;
- a description of the categories of individuals and categories of personal data;
- categories of recipients of personal data;
- details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;
- retention schedules; and
- a description of technical and organisational security measures.

As part of the School's record of processing activities the DPO will document, or link to documentation on:

- information required for privacy notices;
- records of consent;
- controller-processor contracts;
- the location of personal information;
- DPIAs; and
- Records of data breaches.

Records of processing of sensitive information are kept on:

- the relevant purposes for which the processing takes place, including why it is necessary for that purpose;
- the lawful basis for our processing; and
- whether the personal information is retained or erased in accordance with the Retention Schedule and, if not, the reasons for not following the policy.

The School should conduct regular reviews of the personal information it processes and update its documentation accordingly. This may include:

- carrying out information audits to find out what personal information is held;
- talking to staff about their processing activities; and
- reviewing policies, procedures, contracts and agreements to address retention, security and data sharing.

10 PRIVACY NOTICE

The school will issue privacy notices as required, informing data subjects (or their parents, depending on age of the pupil, if about pupil information) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the GDPR including the identity of the data controller and the DPO, how and why the School will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data).

When information is collected indirectly (for example from a third party or publicly available source) the data subject must be provided with all the information required by the GDPR as soon as possible after collecting or receiving the data. The school must also check that the data was collected by the third party in accordance with the GDPR and on a basis which is consistent with the proposed processing of the personal data.

The School will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The School will issue a minimum of two privacy notices, one for pupil information, and one for workforce information, and these will be reviewed in line with any statutory or contractual changes. Follow this link to the GDPR page on KELSI where you will find the model privacy notice(s) for schools to use:

http://www.kelsi.org.uk/school-management/data-and-reporting/access-to-information/the-general-data-protection-regulation-gdpr

11 PURPOSE LIMITATION

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

Personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.

12 DATA MINIMISATION

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role.

The School maintains a Retention Schedule to ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time. Staff must take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with the Schedule. This includes requiring third parties to delete such data where applicable.

Staff must ensure that data subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

13 INDIVIDUAL RIGHTS

Staff as well as any other 'data subjects' have the following rights in relation to their personal information:

- To be informed about how, why and on what basis that information is processed *(see the relevant privacy notice)*
- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request *(see Appendix 1 - Procedure for Access to Personal Information)*
- To have data corrected if it is inaccurate or incomplete
- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where the school no longer need the personal information, but you require the data to establish, exercise or defend a legal claim
- To restrict the processing of personal information temporarily where you do not think it is accurate (and the school are verifying whether it is accurate), or where you have objected to the processing (and the

school are considering whether the school's legitimate grounds override your interests)

- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format
- To withdraw consent to processing at any time (if applicable)
- To request a copy of an agreement under which personal data is transferred outside of the EEA.
- To object to decisions based solely on automated processing, including profiling
- To be notified of a data breach which is likely to result in high risk to their rights and obligations
- To make a complaint to the ICO or a Court.

14 INFORMATION SECURITY

The school will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All staff are responsible for keeping information secure in accordance with the legislation and must follow Sacred Heart's Acceptable Use Policy for staff.

The school will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the **confidentiality, integrity and availability** of the personal data, defined as follows:

- **Confidentiality** means that only people who have a need to know and are authorised to use the personal data can access it.
- **Integrity** means that personal data is accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users can access the personal data when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the school has implemented and maintains in accordance with the GDPR and DPA.

Where the school uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of the school
- those processing data are subject to the duty of confidence
- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of the school and under a written contract
- the organisation will assist the school in providing subject access and allowing individuals to exercise their rights in relation to data protection
- the organisation will delete or return all personal information to the school as requested at the end of the contract
- the organisation will submit to audits and inspections, provide the school with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the school immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

15 INDIVIDUAL RESPONSIBILITIES

15.1 General

At Sacred Heart High School, it is the responsibility of all staff to familiarise themselves with schools' Data Protection Policy, as well as associated platforms provided by the school, and to take all necessary action to ensure that data is kept secure at all times.

During their employment, staff may have access to the personal information of other members of staff, suppliers, pupils, parents or the public. The school expects staff to help meet its data protection obligations to those individuals.

If you have access to personal information, you must:

- only access the personal information that you have authority to access and only for authorised purposes;
- only allow other staff to access personal information if they have appropriate authorisation;
- only allow individuals who are not school staff to access personal information if you have specific authority to do so;
- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the school's policies);

- not remove personal information, or devices containing personal information (or which can be used to access it) from the school's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device
- not store personal information on local drives or on personal devices that are not used for work purposes.

The following protocols do not represent an exhaustive list of how staff should ensure that they act within GDPR but it does set some basic ground rules. Each member of staff is responsible for their own behaviour in this regard.

15.2 Sending emails

Staff should consider carefully before sending any email both internally and externally that contains personal information about a pupil, trainee, parents or other person:

- Are you confident that it is necessary to send the email and are you confident that the email is being directed only at those who need to be aware?
- Have you considered password protecting the information that is being sent? It is important for staff to carefully consider the risk of what they are doing at all times.

Emails containing documents of a personal or sensitive nature must only be sent in encrypted format using the web-based version of Outlook. After creating a new message, you will see an Encrypt button just above the "To" field. Click this to encrypt the email.

15.3 In classrooms

Make sure personal or sensitive information is not displayed on your White Board. Use the Freeze function on your projector or extended your desktop to prevent emails or documents being viewed.

15.4 Remote Connection

If I.T. Support is connecting remotely to perform a task, make sure that you close any documents you do not wish them to see before you accept their remote request.

15.5 Screen Locking

If you leave your computer unused for a period of 5 minutes the system will automatically lock your screen. However if you walk away from your PC, whether it is in an office or a classroom, even for a short time, you should always lock your screen yourself. You can do this by pressing the Windows key + L at the same time

15.6 Replacement for Computer Sticks (USB keys)

USB Mass Storage devices, such as external hard drives and USB keys, should not be used at all whether on or off site. The school has provided all staff with a 'Google drive' for storing teaching resources and a 'OneDrive' for storing all other documents with sufficient storage to use instead of these types of devices.

Whilst on the school network, you can find One Drive just above your network drive list, it is also an app available in your All Programs menu, and you can set up folders in there and save documents to that location to access when you are out of school, just as if you were saving it to a computer stick.

These folders in your One Drive are secure and not accessible to others but you 'can' make a document or group of documents sharable with an individual or group set up within Office 365.

To access your own folders in One Drive outside school, simply login into www.office.com with your school email and network password. You can then select OneDrive from the homepage.

When sharing access within OneDrive make sure any documents of a personal or sensitive nature are password word protected.

Google Drive is accessed by logging into your school Gmail account via a web browser and clicking on the Google apps menu in the top right hand corner.

15.7 Storing Files

Limit potential breaches when storing files on your Google Drive, take time to assess whether they belong in there or on OneDrive. For example, only student resources in Google Classroom drives.

15.8 Hard copies

Physical copies, such as mark sheets or exam analysis, containing data that is personal (first name, surname, SEN details) should be stored securely and disposed of when appropriate using the confidential shredding service provided by the school.

16 STORAGE AND RETENTION OF PERSONAL INFORMATION

Personal data will be kept securely in accordance with the school's data protection obligations.

Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained. Staff should adhere to the KCC Information Management Toolkit for Schools on KELSI with reference to the Record Retention Schedule, available at the following link:

https://www.kelsi.org.uk/__data/assets/word_doc/0004/84667/Information-Management-Toolkit-for-Schools.docx

Personal information that is no longer required will be deleted in accordance with the Schools Record Retention Schedule.

17 DATA BREACHES

17.1 What is a Data Breach?

Under Article 4(12) of the GDPR, a personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. A personal data breach can be broadly

defined as a security incident that has affected the confidentiality, integrity or availability of personal data.

17.2 Types of Data Breach

A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored
- Unauthorised access to or use of personal information either by a member of staff or third party
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Human error, such as accidental deletion or alteration of data
- Unforeseen circumstances, such as a fire or flood
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- Blagging offences where information is obtained by deceiving the organisation which holds it

18 DATA BREACH PROCEDURE

Sacred Heart pays outside consultants at Kent County Council to act as THE schools internal Data Protection Officer (DPO). Outlined below are the steps that must be taken in the event of a suspected data breach.

18.1 Determining if a Breach has Occurred

If a member of staff believes that a breach may have occurred they must immediately notify the school's Data Protection Officer service via the portal below, using the login details sent to you by the school. It's important that you save these where they are quickly accessible to you at all times

https://app.gdpr.school/login

Using this link, simply logs the suspected breach with the school's own Data Officer and they will investigate whether or not it amounts to a formal breach.

In the unlikely event of the portal being unavailable or if the breach has occurred with one of our external data processors, then the report should be made via email and sent to the dpo@sacredh.lbhf.sch.uk address.

Please provide as much information as possible when submitting your report (e.g. Date, time, location of incident, type of data involved, circumstances around the breach, number of individuals affected) and ensure that any affected individual's details, including your own, are not included in the report. The school's DPO will then investigate the report, and determine whether a breach has occurred.

Staff should ensure they inform their line manager/DPO/Head teacher immediately that a data breach is discovered and make all reasonable

efforts to recover the information, following the school's agreed breach reporting process.

During school holidays, staff should follow the same procedure. In times when the school is not in session and there are limited staff onsite, there is potential for our response time to be hindered as a result. In order to mitigate the effects of these factors, the DPO service will have contact details for the Head Teacher, Business Manager and members of the IT support team. The DPO email address will also be monitored by an assigned member of staff.

18.2 Process if Breach is Confirmed

In the event of a breach, the DPO service will alert the Head Teacher and the other members of the Data Breach Response Team when deemed appropriate. The Data Breach Response Team consists of:

- Head Teacher
- Business Manager
- Head of IT
- Lead Safeguarding Officer (only in cases where there may be a safeguard concern)

In the absence of the Head Teacher, the Business Manager will assume the strategic lead of the investigation. The DPO, in conjunction with the appropriate staff, will make all reasonable efforts to contain and minimise the impact of the breach.

Depending on the severity of the breach, the DPO will assess the potential consequences and how likely they are to happen. The DPO will then decide whether the breach must be reported to the ICO.

18.3 Assessing the Need to Report to Information Commissioner

The DPO will consider whether the breach is likely to have a negative impact on people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the Information Commissioner's Office (DPO).

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.

18.4 Reporting to the Information Commissioner

In the event that the ICO needs to be notified, the DPO must do so 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.

18.5 Reporting to Individuals whose data has been breached

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:

- description of the nature of the breach
- the name and contact details of the DPO or other contact point
- a description of the likely consequences of the breach
- a description of the measures taken or proposed to be taken by the School to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

18.6 Reporting to Third Parties

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)

18.7 Review

The DPO and Head teacher or Lead Data Managers will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

19 TRAINING

The school will ensure that staff are adequately trained regarding their data protection responsibilities.

20 CONSEQUENCES OF A FAILURE TO COMPLY

The school takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the school and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under the school's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact your line manager or the school's DPO.

21 THE SUPERVISORY AUTHORITY IN THE UK

Please follow this link to the ICO's website (https://ico.org.uk/) which provides detailed guidance on a range of topics including individuals' rights, data breaches, dealing with subject access requests, how to handle requests from third parties for personal data etc.

22 REVIEW AND RATIFICATION

This policy will be reviewed annually and updated as necessary to reflect best practice or amendments made to the GDPR or DPA.

Mrs M Doyle
Headteacher

John Sills
Chair of Governors

GLOSSARY

Automated Decision-Making (ADM): when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits automated decision-making (unless certain conditions are met) but not automated processing.

Automated Processing: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. profiling is an example of automated processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, which signifies agreement to the processing of personal data relating to them.

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. It is responsible for establishing practices and policies in line with the GDPR. The school is the Data Controller of all personal data relating to its pupils, parents and staff.

Data Subject: a living, identified or identifiable individual about whom we hold personal data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major systems or business change programs involving the processing of personal data.

Data Protection Officer (DPO): the person required to be appointed in public authorities under the GDPR.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (not just action).

General Data Protection Regulation (GDPR): General Data Protection Regulation (*(EU) 2016/679*). Personal data is subject to the legal safeguards specified in the GDPR.

Personal data is any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when the school collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for

example, school workforce privacy policy) or they may be stand-alone privacy statements covering processing related to a specific purpose.

Processing means anything done with personal data, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination or otherwise making available, restriction, erasure or destruction.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal data relating to criminal offences and convictions