OCTOBER 2022

Data Protection

GDPR

Data Protection Officer: Margaret Arksey

POLICY

Swansfield Park Primary School

Introduction

At Swansfield Park Primary School, we required to keep and process personal information about staff members and pupils in accordance with our legal obligations under the GDPR.

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the Local Authority (LA), other schools and educational bodies, and Children's Services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the GDPR.

Organisational methods for keeping data secure are imperative, and we at Swansfield Park Primary School believe that it is good practice to ensure policies are practical and supported by clear written procedures.

This policy complies with the requirements set out in the GDPR, which comes into effect on the 25th May 2018. The government have confirmed that the UK's decision to leave the EU has not affected the commencement of the GDPR.

Legal framework

This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

This policy also has regard to the following guidance:

- ICO (2018) 'Guide to the General Data Protection Regulation (GDPR)'

This policy will be implemented in conjunction with the following other school policies:

- Use of Cameras and Mobile Phones Policy
- IT and Information Security Policy

Applicable data

For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual; including information such as an online identifier, e.g. an IP address or UPN. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data (e.g. key-coded).

Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

Principles

In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- 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; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- 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.

The GDPR also requires that “the controller shall be responsible for, and able to demonstrate, compliance with the principles”.

Accountability

Swansfield Park Primary School will implement appropriate technical and organisational measures to demonstrate that data is processed in-line with the principles set out in the GDPR. The school will provide comprehensive, clear and transparent privacy policies. Records of activities relating to higher-risk processing will be maintained, such as the processing of activities that:

- Are not occasional;
- Could result in a risk to the rights and freedoms of individuals; and/or
- Involve the processing of special categories of data or criminal conviction and offence data.

Internal records of processing activities will include the following:

- Name and details of the organisation;
- Purpose(s) of the processing;
- Description of the categories of individuals and personal data;
- Retention schedules;
- Categories of recipients of personal data;
- Description of technical and organisational security measures; and
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place.

The school will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation;
- Pseudonymisation;
- Transparency;
- Allowing individuals to monitor processing; and
- Continuously creating and improving security features.

Data protection impact assessments will be used, where appropriate.

Data protection officer (DPO)

Swansfield Park Primary School shall appoint a DPO in order to inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws. The DPO shall also monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

Provided that their duties are compatible with the duties of a DPO and will not result in a conflict of interest, an existing employee will be appointed to the position of DPO. This individual will have professional experience and knowledge of data protection law, particularly that in relation to schools and will report to the highest level of management at the school; the head teacher. They shall be free to operate independently and shall not be dismissed or penalised for performing this task. Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed. The GDPR sets out the legal basis or conditions for processing personal data, and – where the data controller is not required to do so to meet its legal obligations – consent of the data subject shall be freely obtained prior to their data being processed. For the avoidance of doubt, the GDPR states that consent is not required when processing of personal data is necessary for:

- Compliance with a legal obligation;
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- For the performance of a contract with the data subject or to take steps to enter into a contract;
- Protecting the vital interests of a data subject or another person; and
- For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. However, this final condition is not available to processing undertaken by the school in the performance of its tasks.

'Special categories of data' as defined by Article 9 of the GDPR – data which is of a racial or ethnic origin, relates to political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data, data concerning health or data concerning a person's sex life or sexual orientation – shall only be processed if the explicit consent of the data subject has been given (unless the reliance on consent is prohibited by EU or Member State law); the processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent; the processing relates to personal data manifestly made public by the data subject; or the processing is necessary for:

- Carrying out obligations under employment, social security or social protection law, or a collective agreement;
- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent;

- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity;
- Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards;
- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional;
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices; and/or
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with article 89(1).

Consent

The consent given by a data subject or their parent / guardian must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes. Consent will only be accepted where it has been freely given, it is specific and is an informed and unambiguous indication of the data subject's wishes. Where consent is given, a record will be kept which documents how and when this consent was given. At Swansfield Park Primary School, we ensure that the means for consent to be given meets the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

NOTE: Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be re-obtained.

Consent can be withdrawn by the individual at any time, and where a child is under the age of 16 (or younger if the law provides it i.e. up to the age of 13), the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child. As a Primary School, this shall apply in all instances with the pupils at Swansfield Park Primary School.

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 on the school website. Should services be offered directly to a child, the school will ensure that the privacy notice is written in a clear, plain manner that the child will understand. 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 identity and contact details of the controller (and where applicable, the controller's representative) and the DPO;
- 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 of criteria used to determine the retention period;
- The existence of the data subject's rights, including the right to withdraw consent at any time, and lodge a complaint with a supervisory authority; and
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

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 supplied at the time the data is obtained. 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 supplied within one month of having obtained the data. However, if disclosure of this data to another recipient is envisaged, this information will be provided beforehand, and – if the data is used to communicate with the individual – the information will be provided, at the latest, when the first communication takes place.

The right of access

Individuals have the right to obtain confirmation that their data is being processed. To this end, they have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. In order to fulfil its obligations under the GDPR, Swansfield Park Primary School will verify to its satisfaction the identity of the person making the request before any information is supplied. When information is supplied, it shall be given free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information. Similarly, where a request is manifestly unfounded, excessive or repetitive, a reasonable fee based on the administrative cost of providing the information will be charged. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

All requests will be responded to without delay and at the latest, within one month of receipt. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary within one month of the receipt of the request. Where a request is manifestly 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 the request is in relation to.

The right to rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified, and where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible. Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to. Requests for rectification will be responded to within one month, and this will be extended by two months where the request for rectification is complex. 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 and to a judicial remedy.

The right to erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Under the following circumstances, individuals have the right to erasure:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;
- When the individual withdraws their consent;
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
- The personal data was unlawfully processed;
- The personal data is required to be erased in order to comply with a legal obligation; and/or
- The personal data has been processed in relation to the offer of an Information Society Services (as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council as any service normally provided for remuneration at a distance by electronic means and at the individual request of the recipient) to a child.

The school retains the right to refuse a request for erasure where the personal data is being processed 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 or exercise of official authority;
- For public health purposes in the public interest;
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes; and/or
- 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, Swansfield Park Primary 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 certain circumstances, as herein defined. 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 personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data;
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual;
- Where processing is unlawful and the individual opposes erasure and requests restriction instead; and/or
- Where the school no longer needs the personal data but the individual requires the data to establish, 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, without hindrance to usability. However, the right to data portability only applies to personal data that an individual has provided to a controller; where the processing is based on the individual's consent or for the performance of a contract; and when processing is carried out by automated means. In all instances, personal data will be provided in a structured, commonly used and machine-readable form, and will be provided free of charge. Where feasible, data will be transmitted directly to another organisation at the request of the individual. However, the school is not required by the GDPR to adopt or maintain processing systems which are

technically compatible with other organisations. In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual concerned.

As with an individual's subject access rights, the school will respond to any requests for portability within one month. Where the request is complex, or a number of requests have been received, the time frame can be extended by two months, but the individual shall be informed of the extension and the reasoning behind it within one month of the receipt of the request. Where no action is taken in response to a request, the school shall, 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 at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information. Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest, direct marketing, and any processing for scientific or historical research and statistics.

However, where personal data is processed for the performance of a legal task or legitimate interests an individual's grounds for objecting must relate to his or her particular situation. In the event of an individual objecting to their data being processed, the school will stop processing their personal data unless the processing is for the establishment, the exercise or defence of legal claims, or – where the school can demonstrate compelling legitimate grounds for the processing – which override the interests, rights and freedoms of the individual. Similarly, where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data, and where personal data is processed for research purposes, the individual must have grounds relating to their particular situation in order to exercise their right to object.

Where personal data is processed for direct marketing purposes, the school will stop processing personal data for these purposes as soon as an objection is received. Under no circumstances can the school refuse an individual's

objection regarding data that is being processed for direct marketing purposes.

Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online or by other electronic means such as email.

Automated decision making and profiling

Individuals have the right not to be subject to a decision when it is based on automated processing or if it produces a legal effect or a similarly significant effect on the individual. The school will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

When automatically processing personal data for profiling purposes, the school will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact;
- Using appropriate mathematical or statistical procedures;
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors; and
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions must not concern a child or be based on the processing of sensitive data, unless explicit consent of the individual's parents/guardians has been obtained and the processing is necessary for reasons of substantial public interest on the basis of EU or UK law.

Privacy by design and privacy impact assessments

The school will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities. Data protection impact assessments

(DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy. DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur. The school will ensure that all DPIAs include:

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

A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals, and a DPIA may be used for more than one project, where necessary. For the avoidance of doubt, high risk processing includes, but is not limited to, the following:

- 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; and
- The use of CCTV.

NOTE: Where a DPIA indicates high risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

Data breaches

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. The head teacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the Information Commissioner's Office (ICO) – as the supervisory authority – shall be informed.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis. However, all notifiable breaches will be reported to the ICO within 72 hours of the school becoming aware. In the event that a breach is

likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly; as such, a 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified. Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned;
- The name and contact details of the DPO;
- An explanation of the likely consequences of the personal data breach;
- A description of the proposed measures to be taken to deal with the personal data breach; and
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects.

NOTE: Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

Data security

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access and will not be left unattended or in clear view anywhere with general access. Digital data is coded, encrypted (for mobile devices) and/or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site. Where data is saved on removable storage or a portable device, the device will be encrypted and kept in a locked filing cabinet, drawer or safe when not in use. Memory sticks or removable hard drives will not be used to hold personal information unless they are password-protected and fully encrypted. All electronic devices used by staff shall be password-protected to protect the information on the device in case of theft, and, where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft (such as through use of Lightspeed MDM). Staff and governors shall not use their personal laptops or computers for school purposes, and all necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

Emails containing sensitive or confidential information are encrypted if there are unsecure servers between the sender and the recipient, and circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients. When sending confidential information by fax, staff will always check that the recipient is correct before sending.

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, such as the use of encryption and keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure that they are allowed to share it, that adequate security is in place to protect it and who will receive the data has been outlined in the privacy notice available on the school website. Swansfield Park Primary School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information shall be supervised at all times.

The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

The school's senior leadership team is responsible for continuity and recovery measures are in place to ensure the security of protected data.

Publication of information

Some data is routinely made available on the school website. This information may include, but is not limited to, policies and procedures, minutes of meetings, annual reports and financial information. Where this data is published, it shall be made available on request. However, Swansfield Park Primary will not publish any personal information – including photographs – on the school website without the permission of the individual and/or their parents. When uploading information to the school website, staff shall be considerate of any metadata or deletions which could be accessed in any documents and images on the site.

CCTV and photography

The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles. The school notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email should CCTV be used. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose. When recorded, all CCTV footage will be kept for six months for security purposes and the senior leadership team is responsible for keeping the records secure and allowing access.

The school will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them. If the school wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent and/or the pupil. To ensure privacy of pupils, names are not used when publishing photographs of pupils in print, video or on the school website. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, such as during school performances, are exempt from the GDPR.

Data retention

No data will be kept for longer than is necessary than to complete the task for which it is collected and 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 in line with NCC guidance, once the data should no longer be retained.

DBS data

All data provided by the Disclosure and Barring Service (DBS) will be handled in-line with data protection legislation; including electronic communication. Any data provided by the DBS shall not be duplicated and 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.

Policy review

This policy is reviewed every two years by the senior leadership team and the head teacher.

This policy has been formally adopted by the governing body.

VERSION HISTORY

VERSION	DATE	DESCRIPTION
Initially adopted	6 June 2019	Adapted into Swansfield Park Primary School
Review	27 May 2021	Minor date amendments
This Review	October 2022	Minor date amendments

APPROVAL AND AUTHORISATION

	NAME	JOB TITLE	SIGNATURE	DATE
Approved	**Jenny Smith**	Head Teacher	J E Smith	
Approved	**Angela Jefferies**	Chair of Governors	A Jefferies	
DATE OF NEXT REVIEW			**May 2025**	

Swansfield Park Primary School
Headteachers:
Mrs J E Smith BSc PGCE,
Mrs A-M Grimes BA(Hons) PGCE