Data Protection Policy

Author: M Spencer	Position: DHT	
Status: [Approved/Draft]	Approved by Governing Body date:	
Last Updated: May 2018	Next Review: May 2019	Version: 1.0

1 Overview

The purpose of this policy is to ensure that the School is committed to compliance with all relevant data protection laws in respect of personal data and to protecting the "rights and freedoms" of individuals whose information the School collects in accordance with the General Data Protection Regulation (GDPR) and other related data protection laws. To that end, Star Primary School has developed, implemented, maintains and continuously improves data protection policies and procedures.

2 Responsibilities

- The School is a data controller and a data processor under the GDPR.
- The Head Teacher and all those throughout the School who are responsible for developing and encouraging good information handling practices.
- The Data Protection Officer (DPO), a role specified in the GDPR, is accountable for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:
  1. Development and implementation of the GDPR as required by this policy; and
  2. Security and risk management in relation to compliance with the policy.

- The School's nominated person has been appointed to take responsibility for the School's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that the School complies with the GDPR, as do staff in respect of data processing that takes place within their area of responsibility.
- The School's nominated person has specific responsibilities in respect of procedures such as the Subject Access Request (SAR) Procedure and is the first point of call for staff seeking clarification on any aspect of data protection compliance before contacting the Head Teacher.
- Compliance with data protection legislation is the responsibility of all members of the School who process personal information.
- The School will ensure appropriate data protection training is provided for all staff.
- Staff are responsible for ensuring that any personal data supplied by them, and that is about them, to the School is accurate and up-to-date.

3 Objectives

The School is committed to complying with data protection legislation and good practice including:

- Processing personal information only where this is strictly necessary for legitimate purposes
- Collecting only the minimum personal information required for these purposes and not processing excessive personal information
- Providing clear information to individuals about how their personal information will be used and by whom
- Only processing relevant and adequate personal information
- Processing personal information fairly and lawfully
- Maintaining an inventory of the categories of personal information processed by the School
- Keeping personal information accurate and, where necessary, up to date
- Retaining personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate purposes
- Respecting individuals' rights in relation to their personal information, including their right of subject access
- Keeping all personal information secure
- Only transferring personal information outside the European Union in circumstances where it can be adequately protected
- The application of the various exemptions allowable by data protection legislation

4 ICO Registration

- The School has notified the Information Commissioner's Office (ICO) that it is a data controller and that it processes certain information about data subjects. The School has identified all the personal data that it processes and this is contained in the Information Asset Register (IAR)
- A copy of the ICO Registration is retained by the Head Teacher and is available to view on the ICO website
- The ICO registration is renewed annually
- The School's nominated person is responsible, each year, for reviewing the details of registration, in the light of any changes to the School's activities (as determined by changes to the IAR) and to any additional requirements identified by means of data protection impact assessments

The policy applies to all staff and interested parties of the School such as data processors. Any serious breach of data protection legislation will be dealt with under the School's disciplinary policy and may also be a criminal offence, in which case the matter will be reported to the Information Commissioner's Office (ICO) or Police. The School is required to report serious data breaches within 72 hours of the incident to the ICO.

When a personal data breach has occurred, the School will establish the likelihood and severity of the resulting risk to individual's rights and freedoms. If it is likely that there will be a risk the ICO must be notified.

Recital 85 of the GDPR explains that…"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

5 Introduction to GDPR

The GDPR replaces the EU (European Union) Data Protection Directive of 1995 and supersedes the Data Protection Act 1998. Its purpose is to protect the “rights and freedoms” of living individuals, and to ensure that personal data is not processed without their knowledge, and that it is processed lawfully.

6 Definitions

Territorial scope – the GDPR applies to all controllers that are established in the EU who process the personal data of data subjects. It applies to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour to data subjects who are resident in the EU.

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose of its data processing activities. The main establishment of a processor in the EU will be its administrative center. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates, to act on behalf of the controller and deal with supervisory authorities.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an 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.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. The School is a data controller.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or predict that person’s performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – 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. There is an obligation on the controller to report personal data breaches to the

supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – The GDPR does not define the age at which a person is considered to be a child. The processing of personal data of a child under 13 years of age in relation to online services is only lawful if parental or guardian consent has been obtained.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

7 Risk Assessment

Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the "rights and freedoms" of natural persons, the School shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

The School has a process for assessing the level of risk to individuals associated with the processing of their personal information. The assessment is known as a Data Protection Impact Assessment (DPIA). The School shall manage any risks which are identified by the DPIA in order to reduce the likelihood of a non-conformance with this policy.

Where, as a result of a DPIA, it is clear that the School is about to commence processing of personal information that could cause damage and/or distress to the data subjects, the decision as to whether or not the School may proceed must be escalated for review to the Head Teacher.

The DPO will, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the ICO.

Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to the School's documented risk acceptance criteria and the requirements of the GDPR.

8 Data Protection Principles

All processing of personal data must be done in accordance with the following data protection principles of the GDPR and the School's policies and procedures are designed to ensure compliance with them.

<u>Personal data must be processed lawfully, fairly and transparently</u>

The GDPR introduces the requirement for transparency whereby the controller has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' "rights and freedoms". Information must be communicated to the data subject in an intelligible form using clear and plain language commonly in the form of a privacy notice.

The specific information that must be provided to the data subject must as a minimum include:

- The contact details of the School
- The contact details of the DPO
- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing

- Who the personal data will be shared with
- The period for which the personal data will be stored
- The existence of the data subject rights
- The categories of personal data concerned
- Is the data transferred out of the EU
- Any further information necessary to guarantee fair processing

Personal data can only be collected for specified, explicit and legitimate purposes

- Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the Information Commissioner as part of the School's GDPR registration.

Personal data must be adequate, relevant and limited to what is necessary for processing

- The School's nominated contact is responsible for ensuring that information, which is not strictly necessary for the purpose for which it is obtained, is not collected.
- All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be approved by the Head Teacher
- The Head Teacher will review data collection methods on a regular basis to ensure that collected data continues to be adequate, relevant and not excessive.
- If data is given or obtained that is excessive or not specifically required by the School's documented procedures, the School's nominated contact is responsible for ensuring that it is securely deleted or destroyed in line with the School's retention schedule.

Personal data must be accurate and kept up to date

- Personal Data that is processed must be reviewed and updated as necessary. No data should be retained unless it is reasonable to assume that it is accurate.
- The Head Teacher is responsible for ensuring that all staff members are trained in the importance of collecting accurate data and maintaining it.
- It is also the responsibility of individuals to ensure that data held by the School is accurate and up-to-date. Completion of an appropriate registration or application form etc. will be taken as an indication that the data contained therein is accurate at the date of submission.
- Staff/Pupils/Others should notify the School of any changes in circumstance to enable personal records to be updated accordingly. Instructions for updating records are contained on the School's website. It is the responsibility of the School to ensure that any notification regarding change of circumstances is noted and acted upon within 1 month.
- The Head Teacher is responsible for ensuring that appropriate additional steps are taken to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.
- The School's nominated contact will review all the personal data maintained by the School on a regular basis, by reference to the IAR, and will identify any data that is no longer required in the context of the registered purpose and will arrange to have that data securely deleted/destroyed in line with School's data retention schedule.
- The School's nominated contact is responsible for making appropriate arrangements that, where third party organisations may have been passed inaccurate or out-of-date personal information, for information about them that the information is inaccurate and/or out-of-date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal information to the third party where this is required.

Personal data must be kept in a form such that the data subject can be identified only as long as is

necessary for processing.

- Where personal data is retained beyond the processing date, it will be held securely in order to protect the identity of the data subject in the event of a data breach.
- Personal data will be retained in line with the School's Records Retention Schedule and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

Personal data must be processed in a manner that ensures its security

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed. Data held by the School is secure, controlled and managed. The School's systems and network are regularly independently tested.

Security controls may be subject to audit and review by independent auditors.

Personal data shall not be transferred to a country or territory outside the European Union 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.

The transfer of personal data outside of the EU is prohibited unless one or more of the specified safeguards or exceptions apply.

Safeguards

An assessment of the adequacy by the data controller taking into account the following factors:

- The nature of the information being transferred
- The country or territory of the origin, and final destination, of the information
- How the information will be used and for how long
- The laws and practices of the country of the transferee, including relevant codes of practice and international obligations
- The security measures that are to be taken as regards the data in the overseas location

Accountability

The GDPR introduces the principle of accountability which states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the GDPR.

Specifically, controllers are required to maintain necessary documentation of all processing operations, implement appropriate security measures, perform DPIAs, comply with requirements for prior notifications, or approval from the ICO and appoint a DPO.

Data subjects' rights

Data subjects have the following rights regarding personal data that is recorded about them:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing

- The right to data portability
- The right to object

Complaints

Data Subjects who wish to complain to the School about how their personal information has been processed may lodge their complaint with the DPO.

If Data Subjects are not satisfied with the outcome of their complaint or the way in which it has been handled, they may also complain directly to the ICO.

Consent

The School understands 'consent' to mean that it has been explicitly and freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the data subject can be withdrawn at any time.

The School understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be active communication between the parties which demonstrate active consent. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

In most instances consent to process personal and sensitive data is obtained routinely by the School using standard consent documents e.g. when a new member of staff signs a contract of employment, or during induction for participants on programmes.

Where the School provides online services to children, parental, or custodial authorisation must be obtained. This requirement applies to children under the age of 13.

Security of data

All Staff are responsible for ensuring that any personal data which the School holds and for which they are responsible, is kept securely and is not under any condition disclosed to any third party unless that third party has been specifically authorised by the School to receive that information and has entered into a confidentiality agreement.

Any third parties working with or for the School, and who have or may have access to personal information, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by the School without having first entered into an agreement which imposes on the third party obligations no less onerous than those to which the School is committed, and which gives the School the right to audit compliance with the agreement.

All personal data should be accessible only to those who need to use it. The School will form a judgment based upon the sensitivity and value of the information in question, but personal data must be kept:

- In a locked room with controlled access
- In a locked drawer or filing cabinet
- If computerised, password protected
- Encrypted if stored on mobile/removable devices

Care must be taken to ensure that PC screens and terminals are not visible except to authorised

members of staff of the School.

Manual records are not to be left where they can be accessed by unauthorised personnel and may not be removed from School premises without explicit authorisation.

Personal data will only be deleted or disposed of in line with the School's Retention Policy. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Storage drives of redundant PCs and mobile devices are to be removed and immediately securely destroyed.

Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site and appropriate security controls implemented.

Security controls may include:

- Data encryption
- Password or PIN protected data
- Secure storage device
- Secure remote access to the data
- Not working in an environment that is not secure or safe
- Not keeping laptops or paper records overnight in a vehicle

Rights of access to data

Data subjects have the right to access any personal data (i.e. data about them) which is held by the School in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by the School, and information obtained from third parties about that person. SARs are dealt with as described in the SAR Procedure.

Disclosure of data

The School must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of the School's business.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the DPO.

Retention and disposal of data

Personal data may not be retained for longer than it is required. Once a member of staff has left the School, it may not be necessary to retain all the information held on them. Some data will be kept for longer periods than others. The School's Retention Policy will apply in all cases.

Disposal of records

Personal data must be disposed of in a way that protects the "rights and freedoms" of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion).

9 Compliance

All staff are expected to comply with the School's policies to the highest standards. If any School employee is found to have breached this policy, they may be subject to the School disciplinary procedure. If a criminal offence is considered to have been committed, further action may be taken to assist in the prosecution of the offender(s).