St Andrew's CE Primary School
Coleman Street
Whitmore Reans
Wolverhampton
WV6 0RH

ICO Registration No: Z8849196

Data Protection Policy

Document History

Version	Date	Description	Author
1.0	25/04/2018	Draft for consultation with school	IG Team CWC

Contents

1. Introduction

St Andrew's CE Primary School (The School) collects and uses different types of information about people with whom it deals and communicates with in order to operate. These include current, past and prospective pupils, parents and guardians of pupils, staff, contractors, suppliers. In addition, it may occasionally be required by law to collect and use certain types of information to comply with the requirements of government departments or UK law.

It is the School's obligation, as Data Controller, to ensure compliance with current Data Protection laws or regulations. This policy applies to all personal data held by the School and includes manual/paper records and personal data that is electronically processed by computer systems or other means such as CCTV systems.

Current applicable legislation includes; The Data Protection Act 2018 and the General Data Protection Regulations 2016/679 (GDPR) detail the requirements and safeguards for personal data.

2. Purpose

The purpose of this policy is to enable the School to:

- Comply with the law in respect of the personal and special category data it holds about individuals.
- Follow good practice in information handling and management.
- Protect pupils of the School, parents/careers of pupils, staff and other individuals who the School holds personal information about.

This policy is part of an Information Governance framework within the School to ensure compliance with current Data Protection law and associated legislation relating to personal information. It applies to the whole life cycle of information, including the collection, use, disclosure, retention and destruction of data.

The School recognises its responsibility to fully implement its' duties in respect of the above and to ensure that all employees understand and can implement all the requirements of the Act and GDPR.

This policy will underpin any operational processes and procedures connected with the principles of Data Protection.

3. Scope

This policy will apply to anyone accessing or using personal or special category (sensitive) information, held by the school.

4. The Policy

Please see **Appendix A** for a list of definitions which are relevant to Data protection and this policy.

4.1 Objectives

The School will:

- Implement fully, the conditions regarding the fair collection and use of personal information;
- Meet its legal obligations to specify the purpose for which information is used;
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that the rights of people about whom the information is held can be fully exercised;
- Handle queries about personal information in a prompt and courteous manner;
- Ensure that there is someone with specific responsibility for data protection in the organisation;
- Ensure that everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Ensure that everyone managing and handling personal information is appropriately trained to do so;
- Ensure that everyone managing and handling personal information is appropriately supervised;
- Ensure that anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
- Ensure that methods of handling personal information are regularly assessed and evaluated;

4.2 Data Protection Principles

The key Principles of Data Protection, included in both the Act and GDPR, that the School must comply with in relation to processing of personal data are as follows. For more detailed information of the procedures to follow to meet these principles please see **(Appendix B):**

	Data Protection Act principles	General Data Protection Regulation principles
Lawfulness	i. Personal data shall be processed fairly and lawfully and according to conditions.	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
Purpose	ii. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Data minimisation	iii. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
Accuracy	iv. Personal data shall be accurate and, where necessary, kept up to date.	Personal data shall be 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.
Storage	v. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; 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. Please see the **Records Management Policy** for more guidance.
Access	vi. Personal data shall be processed in accordance with the rights of data subjects.	The GDPR does not have an equivalent principle. Instead access rights are found separately in Chapter III of GDPR. A further right in relation to compensation is listed under Article 82 of GDPR.

	Data Protection Act principles	General Data Protection Regulation principles
		Please see **Appendix C** for more detail on data rights
Security	vii. 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	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Please refer to the following documents for more guidance.
Overseas transfer	viii. Personal data shall not be transferred to a country or territory outside the European Economic Area 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 GDPR does not have an equivalent principle. Instead overseas transfers of personal data are addressed separately in Chapter V.
Accountability	The 1998 Act does not have an equivalent principle.	The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

4.3 Personal Information Sharing

Any regular sharing of personal information between the School and other agencies will be subject to an information sharing protocol that commitments the partners to an agreed data, transfer process that meets the requirements of the Data Protection Act.

Personal information sharing within the School must comply with the data protection principle on “Purpose”, in that ‘Personal data shall be obtained only for one or more specified or lawful purposes and shall not be processed in a manner incompatible with that purpose’.

4.4 Data Privacy Impact Assessments

A data privacy impact assessment (DPIA) is now mandatory under GDPR legislation. A DPIA will be carried out whenever there are projects, new or changed service activities, or new ICT that could potentially impact on the privacy of individuals. The results of assessments will be reported by exception, for high risks identified, by the Head teacher to the School Governors Board.

4.5 Consent

GDPR now places a higher threshold for using consent as a lawful basis for processing person or special category data.

The correct use of consent should put individuals in control of their personal data, build customer trust and engagement, and enhance the School's reputation.

Where the School has another lawful basis for processing personal data this should be relied upon instead of consent, as consent must only be used where the data subject has a true choice in the processing of their personal data. (See **Appendix B** for other conditions of lawful processing)

Please see **Appendix D** for more information on obtaining and using consent.

4.6 Subject Access Requests

Individuals have the right to access their personal data and supplementary information about how their data is being processed under both the Act, the Bill and GDPR.

Any request for access to personal information must be handled and responded to in a timely manner in line with the requirements of the law.

All staff must be able to recognise a request for personal information and handle it appropriately by escalating this to Lisa Thompson, Headteacher, St Andrew's CE Primary School, Coleman Street, Wolverhampton, WV6 0RH, telephone 01902 558522 to review, log and co-ordinate a response.

Please see **Appendix E** for more information on subject access request procedures.

4.7 Training

Data Protection training will be made available for all School employees.

Training will be made mandatory for individuals who process personal or sensitive data in their day to day roles, based on a training needs analysis and subject to regular review. The training provided is aimed to ensure employees understand their responsibilities for managing data in line with Data Protection Principles.

Training materials will be kept up to date with relevant UK legislation, and will be made available in different formats including face to face and e-learning courses.

4.8 Roles and Responsibilities

Head Teacher

The Head Teacher and The School Board of Governors have overall accountability and responsibility for all aspects of information governance, including data protection. They are responsible for ensuring that the Schools approach is effective in terms of resource, commitment and execution and is being appropriately communicated to staff.

They are required to provide assurance that all risks relating to data protection and information security are effectively managed and mitigated.

They will delegate responsibility for compliance with the Data Protection laws (including the implementation of this policy and other related policies) to the Data Protection Officer and Margot Cox, School Business Manager.

Board of Governors

The Head Teacher and The Board of Governors have overall accountability and responsibility for all aspects of information governance, including data protection.

The Board of Governors will lead and foster a culture that values, protects and uses information for the benefit of both the School and its pupils.

They have overall responsibility to oversee that information threats and data security breaches are identified, assessed and any data breaches managed and escalated appropriately.

They will ensure that the Head Teacher and or nominated Data Protection Officer and the School staff are fully briefed on all information risks and issues faced by the School

Data Protection Officer (DPO)

The DPO's role is to inform and advise the School and those who carry out processing of School data, of their obligations in line with relevant data protection law;

The DPO will:

- Monitor compliance with The Data Protection Act 2018 (The Act) and the General Data Protection Regulations (GDPR) and with the Schools policies in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- Provide advice where requested with regards to the data protection impact assessment (DPIA) and monitor its performance pursuant to Article 35;
- Cooperate with the Supervisory Authority; this being the Information Commissioner's Office (ICO)

- Act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, on any other matter.
- Shall perform their duties in an independent manner with due regard to the risk associated with processing operations; taking into account the nature, scope, context and purposes of processing.

Responsibilities of Managers

All managers are:

- Required to ensure that they (and their staff) understand and adhere to this policy and any associated procedures.
- Responsible for ensuring that staff are informed and updated on any changes made to this policy.
- Identify and report any risks or breaches to the security of personal data processed by the School to their relevant line manager or Head Teacher.
- Must ensure that their staff undertake information governance training and any training in data protection/information security which is specific to their role. Refresher training will be undertaken annually.

Staff

All staff, whether permanent or temporary, are required to:

- Read, understand and accept any policies and procedures that relate to personal data that they may handle during the course of their work.
- Have a responsibility for data protection and are required to adhere to this policy, any associated procedures
- To attend any associated data handling, protecting information, or Data Protection training.
- All staff must understand the main concepts within the legislation, and raise any queries to their line manager or the Head Teacher for advice and guidance.
- Identify and report any risks to the security of personal data processed by the School to their line manager or the Schools DPO.
- Assist their customers/service users to understand their rights and the School's responsibilities in regard to data protection.
- Identify and report any subject access requests to Lisa Thompson, Headteacher, St Andrew's CE Primary School, Coleman Street, Wolverhampton, WV6 0RH, telephone 01902 558522or so that they can be processed in accordance with the law.

5. Policy Review

A review of this policy will take place June 2020, or sooner, in line with any new or changed legislation, regulations or business practices.

6. Monitoring Compliance

Compliance with this policy and related standards and guidance will be monitored as part of the work of the Data Protection Officer and reported to the Board of Governors.

As part of the monitoring and evaluation, an action plan for improvements in Data Protection practices will be formulated as required by the Board of Governors.

Disregard for this policy by employees may be treated as misconduct and a serious breach may be treated as gross misconduct and lead to dismissal. In the case of contractors, partner representatives, agency workers and volunteers, disregard of this policy may be grounds for termination of that relationship with the School.

7. References and School Related Policies and Protocols

This policy should be read in conjunction with:

Specify any other policies you have in the School that link to the DP policy or you want your staff to read in conjunction with this policy.

- Information Governance Policy]
- [Records Management policy and Retention Schedule]
- [Information Security Policy]
- [Wolverhampton Information Sharing 3 Tier framework]
- [Freedom of Information policy]

Appendix A - Definitions

All definitions included in this document cover the definitions listed in:

- The Data Protection Act 2018
- The General Data Protection Regulation (EU) 2016/679

1. Data

"Data" means information which;

- Is being processed electronically i.e. Information systems, databases, including microfiche, audio and video systems (CCTV) and telephone logging systems.
- Is recorded with the intention that it shall be processed by equipment or is being processed wholly or partly by automated means (electronically).
- Is recorded as part of a relevant filing system i.e. manual files and records forming part of a relevant filing system structured either by reference to individuals or criteria relating to individuals.
- Is an accessible record (a health record, educational record, local authority housing record, or local social services record).

2. Relevant filing system

A "relevant filing system" is defined as "any set of information relating to individuals that is stored in a structured manner, or is intended to be contained in a filing system, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible, whether held by automated means or manually and whether centralised, decentralised or dispersed on a functional or geographical basis".

This means any data that is filed in such a way that it can allow ready access to specific information about an individual.

For public bodies such as the School, the Data Protection Act, Bill and GDPR state that any personal information held in a manual (paper) and unstructured way, is still subject to the rules of data protection laws. The School is still required to protect this information under data protection principles. The School is required to apply any data rights that are exercised by an individual to this data. The School is required to find and provide this data in response to an access request.

3. Personal Data

"Personal data" is defined as data, which relates to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come in to the possession of the data controller.

Any information relating to an identified or identifiable natural person ('data subject'); 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
- physical details,
- physiological details,
- genetic details,
- mental health details,
- economic factors,
- cultural or social identity of that natural person;

Personal Data includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual

4. Special Category Data (Sensitive)

The three pieces of legislation that are described in this policy refer to categories of personal data that relate to more private matters of a data subject's life, using different terminology.

- The Data Protection Act uses **"Sensitive Personal Data".**
- GDPR uses **"Special Category"** personal data.
- The Data Protection Act 2018 uses **"Sensitive Processing"**

The following categories of data are covered by all of these laws:

- Racial or Ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Physical or mental health
- Sexual orientation or sex life
- Criminal proceeding or convictions

Special categories of data now covered by GDPR and the Data Protection Act are:

- Genetic data
- Biometric data

5. Processing

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether it is by manual or automated means, on paper or electronic records. Any of the following actions, constitutes processing:

- Collection or obtaining
- Recording
- Use
- Disclosing or transmission of data

- Organising, adapting or altering the data
- Structuring
- Storage
- Retrieval
- Consultation
- Dissemination or otherwise making available
- Alignment or combination of data
- Restriction
- Erasure or destruction

6. Data Subject

A “Data Subject” is the individual who the personal data belongs to, they are the subject of the personal data. either directly or can be identified from it. A data subject must be a living individual.

7. Data Controller/ Controller

“Data Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, that determines:

- Legal basis for collecting data.
- Purpose or purposes that the data are to be used for.
- The way personal data may be processed.
- Which items of personal data to collect.
- Whether to disclose the data, and to who, under what circumstances.
- How long to keep the data.

The contacted details and registration of the “Data Controller” or “Controller” for the data processing that is carried out by the School is available on the Data Protection Public Register here: https://ico.org.uk/esdwebpages/search

Name: St Andrew’s CE Primary School

Registration number: Z8849196

Address: Coleman Street, Whitmore Reans, Wolverhampton, WV6 0RH

8. Data Processor/ Processor

A “Data Processor” is any other authorised natural or legal person, public authority, agency or other body, other than an employee of the School who processes personal or special category data on behalf of the School (The Data Controller).

A data processor can decide:

- What it systems or other methods to use to hold personal data.
- How to store personal data.
- The detail of the security applied to protect the data.
- The means used to transfer, retrieve, delete data.
- The method of adhering to the schedule of how long to keep data.

Examples of data processors are:

- Sub-contractors (those who deliver a service on the School's behalf, such as those who run after school activities, if not directly employed by the School, but associated to the School etc.)
- Professional advisors (external legal advice)
- External IT services or solutions (companies who provide our databases to keep staff, customer or service user data, cloud storage)

9. Recipient

A "recipient", in relation to personal data means any natural or legal person, public authority, agency or another body to whom data are disclosed (including employees or agents) of the School.

However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with UK law shall not be regarded as recipients. The processing of this data by a public authority must be done so in compliance with the applicable data protection rules, considering the purposes of the processing.

10. Third Party

"Third party" is any other natural or legal person, public authority, agency or body, other than:

- The data subject
- The data controller
- Or any processor or other person authorised to process for the data controller

11. Subject Access Request/ Access Request

A "Subject Access Request" is a request to access information that the school holds about the individual himself – the "data subject" - or another individual on behalf of the "data subject". Requests must be validated before any information can be disclosed – please refer to Appendix E.

12. Profiling

"Profiling" - means any form of automated processing of personal data to evaluate certain personal aspects relating to a person, in particular to analyse or predict aspects concerning that person's performance at school or work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

13. Pseudonymisation

“Pseudonymisation” means the processing of personal data in such a manner that the personal data can no longer be attributed back to a specific data subject without the use of additional information, also known as a Key. The Key or additional information that can be used to make the data identifiable again must be kept separately to the data, and must be subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable person.

14. Consent

“Consent” of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes, by a statement or by a clear affirmative action, signifies their agreement to the processing of personal data relating to him or her.

15. Condition for Processing

A condition for processing data is a reason why you would be allowed to use personal data, which is set out under the First Principle of Data Protection (see Appendix B). There is a list of reasons that allow you to process personal data, and a separate list which allows you to process special category/sensitive personal data.

16. Supervisory Authority

Is an independent public authority which is established by UK law. In relation to Data Protection, this is the Information Commissioners Office (ICO).

Appendix B – Data Protection Principles

The GDPR regulation sets out several key principles in relation to how Data Controllers must manage personal information. These are broadly in line with the principles in the DPA. These key data protection principles are now explained in more detail below:

Lawfulness - ***"Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency)."***

To fairly and lawfully process Personal Data:

Processing of personal data shall be considered lawful **ONLY** where one of the following conditions apply. (Formerly Schedule 2 of the Data Protection Act 1998)

a) **Consent:** the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) **Contract:** 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;

c) **Legal Obligation:** processing is necessary for compliance with a legal obligation to which the controller is subject (set out by European Union while we are still a member or UK law)

d) **Vital Interests**: processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e) **Public Task:** 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 controller. The legal basis which underpins this may contain specific provisions to specify the lawfulness of processing, specify data items, data subjects, entities and purpose for disclosure of personal data, limitation of the purpose, storage periods, processing operations and procedures. See chapter 9 of the GDPR legislation for more details on provisions relating to specific processing situations here: https://gdpr-info.eu/chapter-9/.

   The Data Protection Act defines these public tasks carried out in the public interest or in the exercise of official authority as:

   - the administration of justice,
   - the exercise of a function of either House of Parliament,
   - the exercise of a function conferred on a person by an enactment or rule
   - of law, or
   - the exercise of a function of the Crown, a Minister of the Crown or a government department.

f) **Legitimate Interests:** processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (set out by European Union while we are still a member or UK law)

g) Point (f) Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority.

To fairly and lawfully process Special Category (Sensitive) personal data:

With regards to Sensitive Personal Data, in addition to one of the above conditions being met, one of the following (Formerly Schedule 3 of the Data Protection Act 1998) conditions must also be met:

a) **Consent:** the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, unless a law prohibits the processing.

b) **Employment and social security:** processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law

c) **Vital Interests:** processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d) **Legitimate Activity:** 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 and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e) **Data is public:** processing relates to personal data which are manifestly made public by the data subject;

f) **Legal Claims:** processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g) **Public Task:** processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

h) **Health and Social Care:** processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

i) **Public Health:** processing is necessary for 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 quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

j) **Archiving, Scientific and Historical research**: processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of GDPR (set out by European Union while we are still a member or UK law) which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

The legal basis for processing any personal data must be known and a record kept of proof of the Schools processing activities, in order to meet the principle of accountability in GDPR.

To process data in a transparent manner

Organisations are required to provide data subjects with information about how their personal data is processed in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This is done in a Privacy Notice which is made available on the Schools website, or in literature available to those who interact with the School.

Much of the information the School MUST supply is consistent with our current obligations under the Data Protection Act 1998, but there is some further information we are explicitly required to provide under the GDPR regulations.

The information you must supply is determined by whether you obtained the personal data directly from the data subject, or from a 3rd party. See the table below for further information on this.

The following information MUST be included in the Privacy notice:

What information must be supplied?	**Data from data subject**	**Data from 3rd Party**
Identity and contact details of the controller and where applicable, the controller's representative) and the data protection officer	☑	☑
Purpose of the processing and the legal basis for the processing	☑	☑
The legitimate interests of the controller or third party, where applicable	☑	☑
Categories of personal data		☑
Any recipient or categories of recipients of the personal data	☑	☑
Details of transfers to third country and safeguards	☑	☑

Retention period or criteria used to determine the retention period	☑	☑
The existence of each of data subject's rights	☑	☑
The right to withdraw consent at any time, where relevant	☑	☑
The right to lodge a complaint with a supervisory authority	☑	☑
The source the personal data originates from and whether it came from publicly accessible sources		☑
Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	☑	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.	☑	☑

Purpose - ***"Personal data shall collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;"***

Data Protection laws require that the School to consider the purpose of why it processes personal and special category data. The School must consider and document the conditions for processing (these are listed under the first principle above) which apply. The School must specify what data is to be included in this purpose, and document it. The School must also confirm that:

- □ We have reviewed the purposes of our processing activities, and selected the most appropriate lawful basis (or bases) for personal and special category data where appropriate, for each processing activity.
- □ We have checked that the processing is necessary for the relevant purpose, and are satisfied that there is no other reasonable way to achieve that purpose.
- □ We have documented all reasons why this data may be used, and have checked there are no incompatible purposes for processing.
- □ We have included information about both the purposes of the processing and the lawful basis for the processing in our privacy notice.
- □ Where purposes change over time or we have a new purpose, we have checked this is compatible with the original purpose. By thinking about:
    - any link between your initial purpose and the new purpose;
    - the context in which you collected the data – in particular, your relationship with the individual and what they would reasonably expect;

- the nature of the personal data – e.g. is it special category data or criminal offence data;
- the possible consequences for individuals of the new processing; and
- whether there are appropriate safeguards - e.g. encryption or pseudonymisation.

The School is legally obliged to notify the reasons why it collects and uses personal data with the Information Commissioner. Please contact the School for an up to date list of the purposes that the School has notified, or to add a reason to the list.

Data Minimisation - ***"Personal data shall be adequate, relevant and limited to what is necessary (not excessive) in relation to the purposes for which they are processed ('data minimisation')"***

Only the minimum amount of information required to fulfil a specific task (purpose) must be collected and used. Information that is not required for the purposes specified should not be requested unnecessarily.

The School must assess the ways it collects information (on forms and websites etc) to ensure that the fields of information being asked for are truly needed to provide that service or School function. The School must look at the ways it stores that data to ensure that only the data needed to provide a service or function can be seen and used by authorised staff.

The School must try to ensure that for non-direct provision of service or care, data that is processed is pseudonymised or anonymised as far as possible to minimise the use of personal data.

Accuracy - ***"Personal data shall be accurate and where necessary, kept up to date, data this is inaccurate or incomplete must be rectified without delay."***

Every reasonable step must be taken to ensure that all data that the School collects is accurate and where necessary kept up to date. The source of the data is clear so issues can be addressed at source, and where data is shared to third parties the errors are corrected in their systems also.

Regular data quality monitoring should be undertaken by departments on their own databases and systems to identify and correct accuracy issues.

Storage - ***"Personal data processed for any purpose or purposes shall not be kept in a form that identifies the data subjects for longer than is necessary for that purpose or purposes"***

Appendix B – Data Protection Principles

The School must ensure that personal information held, and the purpose for holding it, is reviewed regularly. Data must be held in accordance with retention schedules that specify the period for holding such information, and deleted or archived accordingly. Please refer to St Andrew's CE Primary School - Records Management Policy for further guidance.

Where data can be transformed into sets of data that do not identify any individual, for example where all identifiers are removed and only statistics kept, or where data is pseudonymised so separate records can still be recognised, but the individual who that record relates to cannot be identified, the data can be kept longer than the initial purpose.

Personal data can also be kept for longer periods for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Keeping data longer for these reasons must only be done in line with proper technical and organisational security measures required by the GDPR regulation, so that the rights and freedoms of individuals are safeguarded.

Please refer to the St Andrew's CE Primary School **Records Management Policy** for more guidance on records and retention.

Access - ***"Personal Data shall be processed in accordance with the rights of the data subjects"***

Legislation gives rights to individuals in respect of the personal information the School holds about them. The School must ensure it has appropriate procedures in place to deal with any data rights request it receives.

- Right to be informed
- The right to access
- The right to rectify
- The right to be forgotten
- The right to restrict
- The right to data portability
- The Right to object
- The right to object to profiling or automated decision making
- Right to compensation.

Please see **Appendix C** for more detailed information on Data Rights.

Security - ***"Processed in a manner that ensures appropriate technical and organisational measures are taken to ensure the security of the personal data, including protection against unauthorised or***

unlawful processing and against accidental loss, destruction or damage."

The School must ensure that data is kept securely. This means that the data itself is safe from corruption, deletion, change and physical damage. The School is obliged to offer guarantees of what security measures are in place to safeguard personal information such as implementing "safe haven" type arrangements for the transfer of personal and sensitive data, the secure use of mobile computers, data storage devices and remote access facilities etc. Please refer to the following documents for guidance [Information Security Policy]

Overseas Transfers - ***"Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensure that an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data"***

The movement of personal data and information outside of the UK and EEA (European Economic Area) requires special consideration. The Data Protection Act specifies that transfers outside of the EEA are prohibited unless there are adequate safeguards in place to protect the rights and freedoms of individuals in relation to the processing of information about them.

The School must ensure that personal information is not transferred outside of the UK and the EEA without suitable safeguards. Although the School does not routinely transfer data outside of the UK, there may be occasions where this becomes necessary, for example, where a service user requires personal information about them to be transferred to another country for social care or administrative purposes.

Such requests should be processed by specialist staff, with all due regard to the latest statutory requirements and available guidance from the Information Commissioner's Office (ICO). Transfers of this type should only be undertaken with express consent of the individuals concerned and the documented consent of the Head Teacher and or School Governing Body.

Accountability - ***"*****The controller shall be responsible for, and be able to demonstrate, compliance with the principles.*****"***

Principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance, as it is now specifically stated in the regulation.

The School must put in place governance and reporting measures, proportionate to the scale of processing of personal data, to measure and minimise any data risks, and uphold the protection of data robustly across the organisation.

Appendix B – Data Protection Principles

To demonstrate compliance the School will adhere to approved codes of practice and certification schemes

Appendix C - Data Rights of the individual under GDPR

- **Right to be informed** of data processing, at the time of collecting the personal data from the data subject or another source. This must be in a concise, transparent, intelligible and easy accessible form, using clear and plain language. This must be available in writing or electronic means, or where requested by the data subject in another format. (Privacy Notice). The Privacy notice must be regularly reviewed to ensure it reflects the processing that the School does.
- **The right to access** the personal data held about them, and be provided a copy of the data in a commonly used format (this could be paper or an electronic copy). The School must respond to requests in a timely manner (30 days under GDPR) and in line with the law. Please refer to the **Subject Access Request Guidance** in **Appendix E** for more details of how to deal with these requests.
- **The right to rectify** any inaccurate personal data held about them, taking into account the purposes of the processing, and to have incomplete data corrected by adding a supplementary statement. Data subjects can also take this further to get a court order to have the data corrected.
- **The right to be forgotten**, and ask for data held about them to be deleted where the processing of the personal data is no longer necessary, where there is no overriding statutory or legal reason why the data controller should be holding it any longer, or there is a legal reason why it should be deleted, or where we are relying on consent ONLY to process the data and the person withdraws their consent.
- **The right to restrict** processing of their data for certain purposes, where there is a dispute with the data controller about accuracy, lawfulness or purposes of processing, legal claim. Any processing of the personal data during a time of restriction MUST be done with the consent of the data subject.
- **The right to data portability**, to receive data held about them in a structured, commonly used machine-readable format and have the right to transmit that data to another controller. The right to ask for data to be transmitted directly from one controller to another.
- **The Right to object,** at any time to the processing of their personal data. The data controller MUST NOT continue to process the data if this is for direct marketing. For other processing, the data controller MUST NOT continue to process data, unless they can demonstrate compelling legitimate grounds that override the data subject's rights.
- **The right to object to profiling or automated decision making.** Data subjects have the right to not be included in decisions made about them based solely on automated processing (where a computer makes a decision about them) including profiling. Unless they have signed up to a contract to do so, or the data subject has given explicit consent.
- **Right to compensation.** Any person who have suffered material or non-material damage as a result of an infringement of the GDPR regulations has the right to receive compensation for the controller or processor for the damage suffered.

Appendix D – Consent Guidance

Do we always need to collect consent to use personal information?

The Short answer is no. Articles 6 and 9 of GDPR provide a number of conditions that are lawful reasons for processing personal data. Consent is one of those conditions.

If you can rely on another reason to lawfully process data then you don't need to obtain consent. (see **Appendix B** for a full list of lawful processing reasons)

If you have found that your only condition for processing personal data is consent, GDPR places some obligations on data controllers to ensure that the consent gained is:

- An unambiguous clear affirmative action from the data subject (opt-in)
- Explicit and expressly confirmed, it cannot be implied or assumed.
- Granular consent for different purposes of processing the personal data.
- Separate from any other terms and conditions of service.
- It should NOT be a precondition of service, where possible.
- It must be clearly recorded, so the Data Controller can demonstrate consent if asked.
- Consent must be able to be withdrawn, and detail of how to do so must be provided to the data subject.

The checklist below will help you assess if you are managing consent in the right way under the new GDPR regulations.

When we are asking for consent:

- We have checked that consent is the most appropriate lawful basis for processing.
- We have made the request for consent prominent and separate from our terms and conditions.
- We ask people to positively opt in.
- We don't use pre-ticked boxes or any other type of default consent.
- We use clear, plain language that is easy to understand.
- We specify why we want the data and what we're going to do with it.
- We give individual ('granular') options to consent separately to different purposes and types of processing.
- We name our organisation and any third-party controllers who will be relying on the consent.
- We tell individuals they can withdraw their consent.
- We ensure that individuals can refuse to consent without detriment.
- We avoid making consent a precondition of a service.

- If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place

When we are recording consent:

- We keep a record of when and how we got consent from the individual.
- We keep a record of exactly what they were told at the time.

When we are managing consent:

- We regularly review consent to check that the relationship, the processing and the purposes have not changed.
- We have processes in place to refresh consent at appropriate intervals, including any parental consents.
- We consider using privacy dashboards or other preference-management tools as a matter of good practice.
- We make it easy for individuals to withdraw their consent at any time, and publicise how to do so.
- We act on withdrawals of consent as soon as we can.
- We don’t penalise individuals who wish to withdraw consent

Appendix E – Subject Access Request Guidance

A subject access request (SAR) is where a person (data subject) contacts the School to ask for their own records. All School staff need to be aware of Subject Access Requests and how to deal with them appropriately in a timely manner, as the request could:

- Be received into any School department, or by any employee (Teacher, Lunch time supervisor, volunteer etc.)
- Be received via post, email, telephone to anyone in the School.
- The request for their records could be hidden in correspondence about current ongoing issues, or issues that have closed in the recent past. For example: School meals or school trips, following on from letters the school has sent to parents etc.
- Be worded as “a copy of” documents.
- Be worded as “access to” documents
- Be worded as “I want to know what is recorded/ what you have said about me/my child”.

It is important to recognise these requests and send them immediately to to Lisa Thompson, Headteacher, St Andrew’s CE Primary School, Coleman Street, Wolverhampton, WV6 0RH, telephone 01902 558522 to review, log and action on behalf of the School. This is because from 25th May 2018, under GDPR all subject access requests must be:

- Provided free of charge
- Answered without delay and within 30 days.

Any non-response to a SAR is classed as a breach of the Data Protection Law. The issue can be escalated to the Information Commissioners Office (ICO) as the UK’s supervisory authority to investigate the School, take enforcement action against the School, or issue the School a fine.

Once a request is received by the School, it will be:

- Logged - paper database
- Acknowledged to the requestor in writing.
- The identity of the requestor must be verified using reasonable means Parents/Guardians must prove parental responsibility if this is not clearly known by the School. Consideration to family circumstances must be taken into account e.g. Looked After Children (LAC), Adoption, Domestic Violence, child protection concerns etc.
- Consideration must be given to requests regarding children, especially those over 13 with capacity who are allowed to make their own decision on who their personal details are disclosed to (where no other law overrides this, such as Safeguarding concerns)
- Assigned to to Lisa Thompson, Headteacher,
- For Complex or numerous requests, an extension of a further 2 months can be applied. The School must inform the data subject within 1 month of receipt and explain the extension if we wish to apply an extension.

- Where the request is manifestly unfounded, excessive or repetitive for the same information, the School can charge a reasonable fee taking into account administrative costs, or is allowed to refuse to respond.
- Information will be collected from areas/ records across the School.
- Information will be reviewed and redacted in line with exemptions under Data Protection law.
- The request will be answered in the same format it is received unless otherwise stated by the data subject.
- Closed – once the request has been responded to, the request can be closed and any copies of the information supplied can be held for up to three years, in accordance with the School's records retention schedule.