Data Protection Policy

St Agnes C of E Primary School

Approved by:	Mr Chris Cartwright
Last reviewed on:	September 2022
Next review due by:	September 2023

1. Objectives

1.1. We recognise the need for legal compliance and accountability and endorse the importance of the integrity, availability, and confidentiality and security arrangements to safeguard personal data. We also recognise that there are times that personal data is shared with, and/or received from, other organisations and that this needs to be in accordance with the law.

1.2. This policy sets out the key data protection obligations and accountability to which we are fully committed.

2. Scope

2.1. In order to fulfil its statutory and operational obligations we must collect, use, receive and share personal, special personal and crime personal data about living people, e.g.

- members of the public (adults and children)
- current, past, prospective employees
- clients and customers
- contractors and suppliers
- elected members

2.2. This policy covers all aspects of handling personal data, regardless of age, format, systems and processes purchased, developed and managed by/or on behalf of us and any person directly employed or otherwise by us.

2.3. This policy reflects the commitment to compliant with data protection legislation, particularly the Data Protection Act 2018 and the UK General Data Protection Regulation 2016 (UKGDPR).

2.4. This policy meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

2.5. This policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

2.6. This policy reflects the commitment to be compliant with data protection legislation, particularly the Data Protection Act 2018, the UK General Data Protection Regulation 2016 (UKGDPR).

3. Policy

3.1. **Data Protection Officer (DPO):** We will appoint a data protection officer who will be the key contact for the provision of independent advice on all things data protection. The DPO will provide advice and support when dealing data subject enquiries and communications with the Information Commissioner's Office.

3.1.1. Data Protection Officer on behalf of St Agnes C of E Primary School

Justin Hardy
West Street
Oldham
OL1 1UT

Email: DPO@oldham.gov.uk

3.2. Definitions of personal data:

3.2.1. ***Personal data*** means 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;

In summary, anything and everything that can relate to a living person.

3.2.2. ***Special Personal data*** means 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

In summary, these are the data categories that are subject to additional controls in order to prevent unauthorised collection, use, access etc.

3.2.3. ***Crime data*** means criminal offence data, e.g., alleged commission of offences or proceedings for an offence, (actual or alleged), including sentencing, (other than where it is **USED** for Law Enforcement (LED) functions) by competent authorities within the scope of Part 3 of the Data Protection Act 2018. In other words, statutory functions of the local authority for the purposes of the prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

In summary this type of personal data is subject to specific conditions and controls.

3.3. **Data Protection Principles**: There are six principles which provide the framework for personal data handling and for which the council is accountable for compliance.

Personal data shall be:

3.3.1. (a) processed lawfully, fairly and in a transparent manner

To be lawful an appropriate condition of processing needs to be identified. To be fair and transparent a privacy notice needs to be provided/made available to the data subject whose personal data is being handled and the law specifies what information must be communicated.

3.3.2. (b) processed for an explicit and specific purpose and not processed for other incompatible purposes. Scientific/historical/statistical research is not incompatible and nor is archiving in the public interest

Personal data should only be used for the stated lawful purposes, except where the law permits.

3.3.3. (c) adequate, relevant and limited to what is necessary for the purpose

Ensure that personal data is specific to the stated lawful purpose and is not excessive or unnecessary.

3.3.4. (d) accurate and, where necessary, kept up to date; ensuring that personal data that are inaccurate, are erased or rectified without delay.

Ensure that personal data is correct and that any errors are rectified and where appropriate notified to recipients of the personal data.

3.3.5. (e) keep no longer than necessary for the purpose, but can keep for longer is solely for Scientific/historical/statistical research and archiving in the public interest purposes and is kept securely

Personal data should not be kept longer than necessary, taking into account any legal and operational requirements.

3.3.6. (f) protection of the personal data using appropriate technical or organisational measures.

These measures should be selected on the basis of identified threats and risks to personal data and the potential impact on the data subjects, the council and any third parties who are sources, recipients, or processors of the personal data.

3.4. **Mandatory obligations**: we will ensure that we are appropriately registered with the Information Commissioner's Office (ICO) and create and maintain the mandatory Record of Processing Activities (ROPA), to be made available to the (ICO) upon demand

3.5. **Data Protection Impact Assessments (DPIA)**: are an important tool in ensuring that we integrate data protection by design by default into our technical systems and day to day business operations. This can be done by embedding privacy risk considerations into new (and / or changes to) systems and business processes. A DPIA must take place where it is identified that there is a high risk to the privacy rights and freedoms of a data subject. Examples where these are likely to be required, include, but are not limited to, new systems and processes, new or different uses of personal data. Where a high risk is identified the DPO must be consulted before any new or changed processing is introduced to ensure adequate risk mitigation measures are implemented. Where the recommendations of the DPO are not being considered the Headteacher must approve any acceptance of these risks. Where risks are high and not adequately mitigated a referral to the Information Commissioner's Office (ICO) must be made.

3.6. **Data Collection, use and disclosure**: We handle personal data that has been either collected from the data subject and/or other parties, e.g. other people, public sector and regulatory organisations, private and voluntary sector organisations etc.

We will:

3.6.1. only handle personal data where there is a legal basis to do so.

3.6.2. not unnecessarily rely on consent where an alternative legal basis is available for processing personal data. However, where consent/explicit consent, is the lawful basis, then we acknowledge that for consent to be valid it must be freely given and capable of being withdrawn. Where a particular individual is unable, due to age, capacity or other reasons, to give consent directly, consent will be sought from an appropriate person e.g., parent, guardian, legal representative etc.

3.6.3. provide data subjects with privacy notices that explain how their personal data will be processed and how to exercise their individual data rights.

3.6.4. in the event of a personal data security breach, resulting in a high risk to the data subject(s), to notify the data subjects and / or the ICO as appropriate.

3.6.5. in the event of a data subject exercising their individual data rights, we will assess the request and respond within the statutory timeline and provide a complaints process and Individual Rights Policy.

3.6.6. If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

3.6.7. We will obtain written consent from parents/carers for photographs/videos of children to be used for communication/publicity/marketing materials.

3.6.8. Where we use pupils and/or staffs biometric recognition data eg, cashless school dinners, consent from parents/carers and staff will be sought in advance. An alternative system will be provided for those people who do not wish to participate or later withdraw consent.

3.6.9. We ensure personal data is subject to appropriate retention and security controls taking into account the nature of the data and the information risks. Personal data may be stored for longer periods where it is for archiving in the public interest, historical or scientific research purposes, or as required by legislation or regulatory activity.

3.6.10. ensure that when sharing and disclosing personal data this is undertaken within the parameters of the law to prevent unauthorised access to personal data. A record will be kept and where appropriate information sharing agreements (ISA) will be developed in line with the ICO Data Sharing Code of practice. Where the sharing involves a joint controller relationship, the ISA will identify where appropriate a lead controller responsible for specified processing activities and for managing individual rights. Where appropriate DPIA's will be undertaken in advance of the sharing/disclosure.

3.6.11. when handling health and social care personal data, that the Caldicott Principles and National Data Guardian Standards are observed. If any processing falls within the scope of the national data opt-out we follow the prescribed processed to check if any data subjects have opted out of their data being used for this purpose.

3.6.12. when handling special category, crime conviction and offence data, that we comply with the additional policy requirements necessary to support these particular processing activities in order to demonstrate compliance with the data protection principles and retention policies and ensure inclusion in the Records of Processing Activities (ROPA).

3.6.13. ensure that processing of personal data within our supply chains includes the contractual clauses required by law and that processing is only undertaken in accordance with our instructions as data controller.

3.6.14. not transfer personal data outside of the United Kingdom to countries not covered by the UK adequacy regulations, unless the appropriate safeguards and controls are in place. This may include ensuring a transfer impact assessment has been completed, a contract is in place including the ICO authorised contract clauses, the receiver has a certification under an approved certification scheme, and/or an international data transfer agreement is in place.

3.6.15. provide all staff and governors / trustees with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

3.6.16. to co-operate and provide information to the ICO and other regulatory bodies in pursuance of any investigation or enforcement action.

3.7. **Offences**: The data protection legislation contains specific offences:

3.7.1. It is an offence for a person knowingly or recklessly, without the consent of the data controller, to

- obtain or disclose personal data
- procure the disclosure of personal data to another person
- retain it without the consent of the original data controller
- offer to sell or buy the personal data obtained

3.7.2. It is an offence for a person knowingly or recklessly to re-identify information

3.7.3. that is de-identified personal data without the consent of the controller, or to knowingly or recklessly handle such data.

3.7.4. It is an offence to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the data subject making the request for access or portability would have been entitled to receive.

3.7.5. It is an offence to require a data subject to provide or give access to information obtained via data subject access in relation to health, conviction/caution records for the purpose of recruitment, continued employment, in connection with provision of goods and service to the public. In summary a data subject should not be obliged to make a data subject access request for this type of information as a condition/implied condition of employment or contract.

3.7.6. It is an offence to intentionally obstruct, or give false information to the ICO in the exercise of its powers under information notices and/or warrants.

4. Assessment and monitoring

4.1. An annual assessment of compliance with requirements will be undertaken in order to provide:

- Assurance
- Gap analysis of policy and practice
- Examples of best practice
- Improvement and training plans

4.2. Reports will be submitted to the Governing Body.

5. Supporting policies

5.1. This policy must be read alongside the following supporting policies:

- Individual Rights Policy
- Data Subject Access Policy
- DPIA Policy
- Personal Data Sharing Policy
- Special and Crime Personal Data Policy

6. Authority for this policy

6.1. The Governing Body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

6.2. The Headteacher acts as the representative of the data controller on a day-to-day basis and is responsible for the approval of this policy.

6.3. The Data Protection Officer will be the key contact for the provision of independent advice on all things data protection. The DPO will provide advice and support when dealing data subject enquiries and communications with the Information Commissioner's Office.

.