Appropriate Policy Document

December 2023

Weaver Trust

Inspire - Believe - Achieve

1. Introduction

1.1. The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

1.2 When processing personal data, Weaver Trust will comply with the requirements of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA) and any associated legislation.

2. Purpose of Processing Special Category Data

2.1 The UK GDPR defines special category data as personal data that relates to:

- Racial or ethnic origin.
- Political opinions.
- Religious and philosophical beliefs.
- Trade union membership.
- Genetic data.
- Biometric data for the purpose of uniquely identifying a natural person.
- Data concerning health.
- Sex life and sexual orientation.

2.2 Weaver Trust may be required to process special category data relating to both pupils and staff for a variety of purposes. This may include processing:

- racial or ethnic origin data (as part of school census);
- data concerning religious beliefs (as part of holiday planning or where there are links with religious or faith-based organisations);
- biometric data for identification (where an IT, security or catering system uses it); and
- data concerning health (i.e. medical data).
- data required for employment purposes (such as undertaking DBS checks of staff or volunteers);
- family situation (including social services or local authority involvement);
- safeguarding information;
- learning information (such as behaviour and special education needs); and
- financial and funding information (including pupil premium and school meals).

2.3 Whereas some details listed here do not automatically qualify as special category under the definition provided by the UKGDPR, we believe their possible sensitivity warrants inclusion in this list as a demonstration of our commitment to ensuring it is handled securely and responsibly.

2.4 The special conditions under UKGDPR which allow for the processing of special category personal data as identified by Weaver Trust and in line with the DPA 2018 are:

- Article 9(2) (b) – for employment, social security and social protection purposes - where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on Weaver Trust or the data subject in connection with employment, social security or social protection. Examples of our processing may include staff sickness absences.
- Article 9(2) (g) – for substantial public interest purposes. Our processing of sensitive personal data in this context is for the purposes of substantial public interest and is necessary for the carrying out of our role in providing a balanced and broadly based curriculum which promotes the moral, cultural, mental and physical development of pupils at Weaver Trust and society as a whole, and prepares pupils for the opportunities, responsibilities and experiences of later life. This includes such instances of providing counselling services and addressing child safeguarding issues and supporting those with specific disabilities or medical conditions.
- Article 9(2) (h) – for health and social care purposes. Where processing is required as part of our responsibilities in relation to health or social care provision. For example, we engage with both the NHS and local authority in relation to the wellbeing of our pupils.
- Article 9(2) (i) – for public health purposes. For example, where we are required to collect or process medical information in line with public health requirements to address public health concerns.
- Article 9(2) (j) – for archiving, research and statistics purposes – where we are required to provide specific data for statistical analysis or research to the likes of the Department for Education.

2.5 We may also process additional categories of special category personal data (where additional conditions are not required) in line with the following conditions:

- Article 9(2) (a) – explicit consent has been given - In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing. Examples of our processing include dietary requirements and health information we receive for those who require a reasonable adjustment for example in relation to meals.
- Article 9(2) (c) – for vital interests - where processing is necessary to protect the vital interests of the data subject or of another natural person. An example of our processing would be using health information about a member of staff or pupil in a medical emergency.

- Article 9(2) (e) – made public by the data subject – where an individual has clearly made available information relevant to our ongoing relationship with them or their child or to allow us to make reasonable adjustments in our dealing with them, for example, addressing accessibility issues.
- Article 9(2) (f) – for defence of legal claims - Examples of our processing include processing relating to any employment tribunal or other legal claims.

3. Data Protection Act 2018

3.1 Schedule 1 of the Data Protection Act 2018 establishes conditions that permit the processing of the special categories of personal data and criminal convictions data. The Schedule is split into four parts:

- Part 1 – Conditions relating to employment, health and research
- Part 2 – Substantial public interest conditions
- Part 3 – Additional conditions relating to criminal convictions
- Part 4 – Appropriate policy document and additional safeguards

Schedule 1 of the Data Protection Act 2018 establishes conditions that permit the processing of the special categories of personal data as follows:

- The processing of the special categories of personal data meets the requirements in points (b), (h), (i) or (j) of Article 9(2) of the UKGDPR if it meets one of the conditions listed in Part 1 of Schedule 1.
- The processing of the special categories of personal data meets the requirement in point (g) of Article 9(2) of the UKGDPR if it meets one of the conditions listed in Part 2 of Schedule 1.

3.2 This Appropriate Policy Document will cover all processing of special category personal data carried out by Weaver Trust for which all of the following conditions are met:

- we (data controller) are processing personal data which is the subject of Articles 9 or 10 of UK GDPR.
- we (data controller) are processing this personal data in reliance of a condition listed in Parts 1, 2 or 3 of Schedule 1 of the DPA.
- the condition listed in Parts 1, 2 or 3 of Schedule 1 includes a requirement for the data controller to have an Appropriate Policy Document.

4. Schedule 1 Conditions That Are Relevant to Weaver Trust.

4.1 Schedule 1, Part 1 conditions for processing in connection with employment, health and research that are relevant to us are:

- **(Paragraph 1) Employment, social security and social protection:** Processing necessary for the purposes of performing or exercising obligations or rights of the controller or the data subject under employment law, social security law or the law relating to social protection.
- **(Paragraph 2) Health or social care:** Processing necessary for health or social care purposes.

4.2 Schedule 1, Part 2 conditions for processing in the substantial public interest that are relevant to us are:

- **(Paragraph 6) Statutory and government purposes:** Processing necessary for the exercise of a function conferred on a person by enactment or the exercise of a function of the Crown, a Minister or a government department.
- **(Paragraph 8) Equality of opportunity or treatment**: Processing necessary for identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people with the view to enabling such equality to be promoted or maintained.
- **(Paragraph 10) Preventing or detecting unlawful acts -** Processing data concerning any identified or suspected unlawful act including the provision of such data to investigating agencies.
- **(Paragraph 11) Protecting the public against dishonesty etc. -** Processing data concerning dishonesty, malpractice or other improper conduct in order to protect the local community, carrying out investigations and disciplinary actions relating to our employees, assisting other agencies in connection with their regulatory requirements.
- **(Paragraph 16) Support for individuals with a particular disability or medical condition -** To provide appropriate support or services or raise awareness of a disability or medical condition in order to deliver appropriate services and educational support.
- **(Paragraph 17) Counselling etc. -** For the provision or identification of the need for confidential counselling, advice or support or of another similar service provided confidentially.
- **(Paragraph 18) Safeguarding of children and individuals at risk -** Protecting vulnerable children and young people from neglect, physical, mental or emotional harm, identifying individuals at risk and obtaining further support for children and individuals at risk by sharing information with relevant agencies.
- **(Paragraph 24) Disclosure to elected representatives -** Assisting elected representatives such as local government Councillors and Members of Parliament with requests for assistance on behalf of their constituents.

4.3 We may process personal data relating to criminal convictions or offences in connection with statutory functions or as part of recruitment and employment checks. We process criminal offence data for the following purposes in parts 1 and 2 of Schedule 1:

- **Paragraph 1** – employment, social security and social protection
- **Paragraph 6(2)(a)** – statutory, etc. purposes

5. Procedures for Securing Compliance Within Article 5 of the General Data Protection Regulation and Data Protection Act 2018

5.1 Article 5 of the GDPR states that personal data shall be:

- processed lawfully, fairly and transparently

- collected for specific and legitimate purposes and processed in accordance with those purposes
- adequate, relevant and limited to what is necessary for the stated purposes
- accurate and, where necessary, kept up-to-date
- retained for no longer than necessary, and
- kept secure

5.2 In addition, Article 5 requires that the data controller shall be responsible for, and able to demonstrate compliance with, these principles (the accountability principle).

5.3 Our Data Protection Policy sets out requirements for the data protection principles to be complied with when processing personal data. Our Data Protection Officer ensures that the data protection principles are applied and that we can be held accountable for the personal data it processes.

5.4 When processing special category data, the following procedures are used to ensure compliance with the data protection principles:

- **Principle A - lawful, fair and transparent**
  - Personal data shall be processed lawfully, fairly and in a transparent manner. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1.
  - We will:
  - provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice, staff privacy notice and this policy document.
  - ensure that personal data is only processed where a lawful basis applies
  - will ensure that data subjects are not misled about the purposes of any processing
- **Principle B - collected for specific and legitimate 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.
  - only collect personal data for specified, explicit and legitimate purposes, and we will inform data subjects what those purposes are in a privacy notice
  - not use personal data for purposes that are incompatible with the purposes for which it was collected. If we do use personal data for a new purpose that is compatible, we will inform the data subject first
- **Principle C - adequate, relevant and limited to what is necessary**
  - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
  - We collect personal data necessary for the relevant purposes and ensure it is not excessive.

- The information we process is necessary for and proportionate to our purposes.
- Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.
- We will only collect the minimum personal data that we need for the purpose for which it is collected. We will ensure that the data we collect is adequate and relevant.
- Will employ the use of Data Protection Impact Assessments to ensure proposed processing is not excessive.
- Where possible, anonymisation or pseudonymisation are used.

- **Principle D - accurate and, where necessary, kept up-to-date**
  - Personal data shall be accurate and, where necessary, kept up to date.
  - We will take particular care to do this where our use of the personal data has a significant impact on individuals.
  - Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay.
  - If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.
- **Principle E - retained for no longer than necessary**
  - 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.
  - We will only keep personal data in identifiable form as long as is necessary for the purposes for which it is collected, or where we have a legal obligation to do so. Once we no longer need personal data it shall be deleted or rendered permanently anonymous.
  - We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs.
  - Retention periods are based on legal requirements to retain data and consideration of the needs of data subjects through data protection impact assessments.
  - Our retention schedule is reviewed regularly and updated when necessary.
  - Retention periods are set out in our Retention and Disposal Schedules and are published in our Records of Processing Activities Register and Privacy Notices
- **Principle F – integrity and confidentiality (security)**

- 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.
- We will ensure that there appropriate organisational and technical measures in place to protect personal data.
- Technical security controls such as encryption are employed to secure sensitive information within systems.
- Role-based access controls are implemented to restrict access to sensitive data.
- Where possible, anonymisation or pseudonymisation are used to reduce the risk of sensitive data being compromised.
- Hard copy information is processed in line with our security procedures.
- The systems we use to process personal data allow us to erase or update personal data at any point in time where appropriate.

6. Accountability Principle

6.1 In order to demonstrate compliance with the Accountability Principle, we have implemented the following measures:

- We keep a record of all our personal data processing activities
- We carry out a Data Protection Impact Assessments where required
- We have appointed a Data Protection Officer
- We have in place internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection law
- All employees receive annual data protection and information security training
- We undertake regular data protection audits
- We maintain logs of security incidents, data protection rights requests and details on information sharing with partners.

7. Retention and Destruction of Personal Data

7.1 Personal data is held and disposed of in line with our Record Retention and Disposal Schedules.

7.2 When disposing of information, we make sure this is carried out securely by using physical destruction methods as well as electronic data deletion.

7.3 Our Record of Processing Activities register contains details of the retention periods for our data processing activities, together with information on the lawful basis for processing this data. If information is not retained or deleted in line with the policy then the reason is recorded in the Record of Processing Activities.

8. Responsibility for the Processing of Special Category and Criminal Data

8.1 All employees are required to comply with our policies when processing personal data and to ensure that any processing of the personal data is carried out legally, fairly and transparently. Senior staff are responsible for ensuring that systems and processes under their control comply with current data protection legislation and that personal data is processed in accordance with the data protection principles

9. Further Information

9.1 For further information about our compliance with data protection law, please contact the Data Protection Officer by:

- Email: gdpr@imperosoftware.com
- By post:
  Philip Crilly,
  Impero
  Seventh Floor, East West,
  Tollhouse Hill,
  Nottingham
  NG1 5FS