

# **Derby Polish Supplementary School (DPSS) Data Protection Policy**

## **Introduction**

Derby Polish Supplementary School (DPSS) is fully committed to compliance with the requirement of processing all Personal Data (including Special Categories of Personal Data) about Data Subjects in accordance with the Data Protection Act 2018, which implements the General Data Protection Regulation 2016/679 (GDPR) standards.

DPSS will therefore follow procedures that aim to ensure that all volunteers, participants, members, employees, contractors, agents, consultants, partners or other servants of DPSS who have access to any personal data held by or on behalf of DPSS, are fully aware of and abide by their duties and responsibilities under the Act.

## **Statement of Policy**

In order to operate efficiently, DPSS has to collect and use information about people with whom it works and whom it serves. These may include members of the public, current, past and prospective volunteers, participants, members employees and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means there are safeguards within GDPR to ensure this. DPSS regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between DPSS and those with whom it interacts. DPSS will ensure that it treats personal information lawfully and correctly. To this end DPSS fully endorses and adheres to the Principles of Data Protection as set out in the General Data Protection Regulation.

## **The Principles of the General Data Protection Regulations**

GDPR stipulates that anyone processing personal data must comply with Six Data Protection Principles. These Principles are legally enforceable. The Data Protection Principles set out in GDPR state that data must be:

1. processed fairly, lawfully and in a transparent manner;
2. collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes;
3. adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed;
4. accurate and, where necessary, kept up to date – every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay
5. kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data is processed; and
6. processed in a way that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

An overarching principle of GDPR is that DPSS Data Controller must be able to demonstrate compliance with the six principles.

**Personal data** means data that relates to a living individual who can be identified –

a) from those data, or

b) from those data and other information which is in the possession of, or is likely to come into the possession of DPSS and includes factual information (e.g. name, date of birth), an expression of opinion about the individual (a performance appraisal) and any indication of the intentions of the data controller or any other person in respect of the individual.

**Special Categories of Personal Data (previously called sensitive personal data)** means information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexuality. It also includes genetic and biometric data. Special Categories of Personal Data can only be processed under strict conditions and such processing will usually, although not always, require the explicit consent of the Data Subject.

## **Types of information covered by GDPR**

Register or electronic record of trustees, volunteers, pupils, parents/guardians, detailing name, address, telephone number and other personal details:

Registers of trustees, volunteers, employees, pupils, parents/guardians.

Training and advancement records.

Information about trustees/ volunteers/ pupils at events (e.g. trips, excursions, conferences, training events).

Information on donors and Gift Aiders.

Photographic information.

CCTV images.

**NOTE:** Care should be taken to ensure that only factual information is held – adverse comments based on personal opinion should be avoided.

## **Privacy Notice**

When any Personal Data is collected from an individual, they must be provided with a Privacy Notice. The Privacy notice provides information about what, why and how information is processed.

## **Handling of personal and sensitive information**

DPSS will, through appropriate management:

- a) collect and process appropriate personal information only to the extent that it is needed to fulfil the legitimate activities of DPSS, to protect the vital interests of an individual or to comply with legal requirements,
- b) ensure the accuracy of information used
- c) apply checks to determine the length of time information is held,
- d) take appropriate measures to safeguard personal information held both in hard copy and electronic form,
- e) ensure that the rights of people about whom the information is held can be fully exercised under the GDPR. This includes
  - I. the right to be informed that processing is being undertaken

II. the right of access to one's personal information (generally within 1 month of receipt of request) III. the right to correct, rectify, block or erase information regarded as wrong information.

## **Security**

DPSS personnel who collect and process personal data will:

Take reasonable steps to ensure hard copy data is stored securely to prevent accidental loss or damage to information

Ensure electronic data is securely stored and where necessary password access controlled

Be clear about who is responsible at all levels for ensuring information security

Ensure archive records are stored under lock and key

Destroy data securely once it is no longer required for its intended use

Ensure any data stored centrally will only be removed with prior authorisation from the relevant Data Administrator. A document removal register will be kept.

Regular training and advice should be given to ensure all DPSS personnel handling personal and sensitive information apply the basic principles of data protection

## **Implementation**

The board of Trustees should ensure policies are kept up to date and accessible to volunteers, pupils, parents/guardians. Trustees should ensure regular training is undertaken and that DPSS directives are met.

Policy adopted by the Trustees of DPSS on 20<sup>th</sup> March 2020.