UK General Data Protection Regulation Policy Document

Our Commitment:

We are committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller, the handling of such data in line with the data protection principles (see below) and the Data Protection Act (DPA).

This policy meets the requirements of the:

The Data Protection Act 2018 (DPA 2018) and UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020.

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR.

Data protection legislation shall be monitored and implemented to remain compliant with all requirements.

Article 6 Lawfulness of processing

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;

Article 9 Processing of special categories of personal data

1. Processing of 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 shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

1. (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

The requirements of this policy are mandatory for all staff employed by us and any third party contracted to provide services.

If personal information meets the above criteria, then individuals who have personal information held by us will be made aware of the personal information and the criteria for holding the information in the 'Information Audit' document, located on our website.

Roles:

Our contact details for the Data Controller: Ruth Hawker, Plumsun Ltd.
Contact details can be found on the website: www.plumsun.com

The Data Controller is the person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed.

All staff will treat all information in a confidential manner and follow the guidelines as set out in this document.

Any Data Processors, processing data on behalf of us (i.e. external organisations) will confirm that they are achieving their obligations under the UK GDPR Regulations, and are registered with the ICO.

Roles under UK GDPR can be found on the ICO Website.

Training:

We are committed to ensuring that staff are aware of data protection policies, legal requirements.

Notification:

Data processing activities and persons responsible will be registered with the Information Commissioner's Office (ICO) as required by the ICO. Details are available from the ICO: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Breaches of personal or sensitive data shall be notified to the individual(s) concerned and the ICO as specified in the UK GDPR Regulations.

Personal and Sensitive Data:

All data within our control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be those published by the ICO for guidance.

Principles:

Under the UK GDPR, the data protection principles set out the main responsibilities for organisations.

Article 5 of the UK GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) 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;

e) 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 subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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."

Article 5(2) requires that:

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

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.

The need for consent:

We will ask for consent to hold and process personal information if there is no lawful basis for doing so (see article 6 and Article 9 above).

Data Breaches:

All data breaches must be immediately reported to the Data Controller.

The Data Protection Controller will assess whether the breach needs to be reported to the ICO and/or individuals concerned.

The Data Controller will make any necessary reports.

Immediate Action will be taken to review how the breach has occurred, and to make any necessary changes to procedures to ensure that the same problems do not arise in the future.

Protection Impact Statements:

We will evidence the thought and decision making process about data protection when designing any processes in school which involve personal data.

A Data Protection Impact Statement (DPIA) is needed when:

- New Technology is being deployed
- A profiling operation is likely to significantly affect individuals
- There is processing on a large scale of the special categories of data ('special categories' as specified in UK GDPR guidance)

Individuals Rights:

Individuals have the right to:

- Be informed about what data is being held (Information Audit Document published on the school website).
- Be informed about how and why the data is being processed (Information Audit Document published on the school website).
- The right to access any data that is being held (see Subject Access Requests below).
- The right to request that any data is erased (see Subject Access Requests below).
- The right to restrict processing.
- The right to data portability (that the individual can transport the data held about them to another service) if the data is held by automatic means.
- The right to object to the way data is being held or processed.
- The right not to be subject to automated decision-making.

The individual can write to us regarding requests for data to be erased, to restrict processing, to data portability, to not be subject to automated decision-making, or the right to object to the way data is being held or processed.

Biometric Data:

As well as adhering to GDPR regulations in respect to sensitive data, the school will also adheres to DfE Guidance 'Protection of biometric information of children in schools and colleges' March 2018. This section is referred to as the schools statutory biometric policy.

The school:

- Treats the data collected with appropriate care and must comply with the data protection principles as set out in the General Data Protection Regulations.
- Where the data is used as part of an automated biometric recognition system, the school complies with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.
- The school ensures that each parent of a child is notified of the school's intention to use the child's biometric data as part of an automated biometric recognition system.

- The written consent of at least one parent will be obtained before the data is taken from the child and used. This applies to all pupils under the age of 18. In no circumstances will a child's biometric data be processed without written consent.
- The school will not process the biometric data of a pupil (under 18 years of age) where:

  a) the child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;

  b) no parent has consented in writing to the processing; or

  c) a parent has objected in writing to such processing, even if another parent has given written consent.

- The school must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.

The biometric information will only be held as long as it is relevant to do so. Biometric information is included the schools information audit, which is publically available.

Sharing of Information with Third Parties:

There may be circumstances where we are required either by law or in the best interests of our customer to pass information onto external authorities, medical practitioners in the case of an emergency situation. These individuals and authorities have to adhere to data protection law and have their own policies relating to the protection of any data that they receive or collect.

Data Access Requests (Subject Access Requests):

All individuals whose data is held, has a legal right to request access to such data or information. We shall respond to such requests within 30 days.

They should be made in writing to the Data Controller, who may delegate the request (as specified in their role above).

will acts as a contact point for data subjects and the supervisory authority.

No charge will be applied to process the request.

There is a right to appeal to the ICO upon dispute of a decision.

Right to be Forgotten:

Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped, and all their personal data is erased by us including any data held by contracted processors.

Photographs and Video:

Due to carrying out their public duty, the school does not ask for consent from parents when making decisions to use pictures and social media to promote the educational progression of pupils for parents. It also forms evidence of educational attainment for Ofsted and the DfE. However, the school does encourage parents to raise any safeguarding concerns to the school, and staff will respond in a proactive manner.

Photographs and social media are used to ensure that when on visits, evidence of pupil's educational attainment is recorded. This is for educational use only and informs the parents of students' progression. The school takes safeguarding concerns seriously, and so a statement reflects this, should there be any concerns regarding their pupils.

The Information Audit and Privacy Notice provides information regarding the use of photographs used on the website and electronic newsletters.

Photographs and videos are only captured for educational purposes and are not shared with external parties.

Location of Information and Data:

Personal data is mainly held electronically, on servers owned only by Plumsun. They are located within the UK.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the premises, unless the Data Controller has provided permission to do so. If there is no other way to avoid taking a paper copy of data off the premises, the information should not be on view in public places, or left unattended under any circumstances.

- Unwanted or duplicated paper copies of data, sensitive information or files will be shredded. This also applies to handwritten notes if the notes reference any other staff member or customer name.

- Care must be taken to ensure that printouts of any personal or sensitive information are not left in sight of other staff or customers.

- If information is being viewed on a PC, staff will ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.

- Computers will also be encrypted if it viable to do so. The data should not be transferred from computers or USB onto any public computers.

- These guidelines are clearly communicated to all staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Data Security:

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them. Risk and impact assessments shall be conducted in accordance with guidance given by the ICO and in compliance with the Data Protection Regulations (UK GDPR).

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance. The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data.

Data Disposal:

We recognise that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk. All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services. All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process. Disposal of IT assets holding data shall be in compliance with ICO guidance. Paper will be shredded on site.

Our contact details for the Data Controller:

Ruth Hawker, Plumsun Ltd

Signed

Chair of Governors _____

Date 26/03/2024