General Data Protection Regulation Policy 2020

1.Aims

Goldstone Federation aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the **General Data Protection Regulation (GDPR)** and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. This policy applies to all personal data in paper or electronic format and is based on guidance published by the Information Commissioner's Office (ICO).

In addition, 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. Roles and responsibilities

Our schoosl process personal data relating to parents, pupils, staff, governors, visitors and others and therefore acts as a **Data Processor.**

2.1 The member(s) of staff responsible as **Data Controller** is Rachael Williams (Executive Headteacher) and is registered with the ICO. Registration will be reviewed annually or as otherwise legally required. The Board of Governors also act as Data Controllers and have overall responsibility for ensuring that the school complies with data protection obligations.

2.2 This policy applies to all volunteers and staff employed by the school and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.
Staff are responsible and have received training for the following:

- Collecting, storing and processing personal data for data subjects (pupil and parents).
- Informing the school of changes to their own personal data.
- Contacting the DPO or Head when in need of advice, guidance or to report a data breach.

2.3 The **Data Protection Officer (DPO)** is Nicola Tidball and is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law and reporting to the Board of Governors. The DPO is the first point of contact for individuals whose data the school processes and for the ICO.
DPO Contact details: tidball.n@hinstock.shropshire.sch.uk

The school will provide the DPO with the necessary time and resources to enable them to meet their GDPR obligations.

3. Data protection principals

All data within either school's 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.
Data usage has been analysed and an Information Asset Register identifies what data is held by the school and how it is used.

The principles say that data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure
- Not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection of the personal information.

4. Collecting personal data

Personal data will only be processed within the lawful bases to do so under data protection law as follows:

- To **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- To **comply with a legal obligation**
- To ensure the **vital interests** of the individual e.g. to protect someone's life
- So that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- For the **legitimate interests** of the schools or a third party (provided the individual's rights and freedoms are not overridden)
- When the individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

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).

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual's data. Privacy notices will be issued for all new pupils and as part of staff and governor induction processes.

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 (DPIA) shall be conducted in accordance with guidance given by the ICO.

5. Sharing personal data

The intention to share data relating to individuals to an organisation outside of our schools shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared safely and securely with external parties in circumstances where it is a legal requirement to provide such information.

The schools will only appoint suppliers or contractors who can provide sufficient guarantee that they complywith data protection law and a data sharing agreement will be established.

6. Data security and storage of records

The schools will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss or damage.

Paper-based records and potable electronic devises that contact personal data stored securely when they are not in use.
Staff have been trained in the secure storage of data off and on site when not in use, including the use of encryption and for electronic devices and the need for regular password change. Encryption software is used to protect all portable devices and removable media.

7. Data disposal

When personal data is no longer required, it will be deleted or anonymised. This will be done in accordance with the school's Record Retention Schedule (appendix 1), guided by the DfE.

The schools 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 shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

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. Disposal of IT assets holding data shall be in carried out in compliance with ICO guidance.
The school has identified a qualified source for disposal of IT assets and collections as follows:
www.stonegroup.co.uk/contact/book-recycling-collection/

la. Subject Access Requests (SARs)

All individuals, whose data is held by the federation, have a legal right to request access to such data orinformation about what is held. Due to the age limit of the school, parents or carers of pupils may begranted access without the express permission of the pupil.

Subject access requests must be submitted in writing to the DPO and the school will respond within one month of receipt.

The schools withhold the right to refuse a Subject Access Request if it is deemed unfounded or excessive and charge a reasonable administration fee if necessary. In this instance, the individual will be informed and advised of their right to complain to the ICO.

Individuals have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under- which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Parents, or those with parental responsibility, also have the right to free access to their child's educational record within 15 school days of receipt of a written request.

9. Photographs and Videos

As part of each school's activities, we may take photographs and record images of individuals within the school. We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/ carer and pupil.

Consent can be refused or withdrawn at any time and appropriate disposal will be carried out in the line with the ICO guidelines.

Further information can be found in the school's 'Telephone Calls, Mobile Phone, Camera and Video Usage' policy.

10. Personal data breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. The school will make all reasonable endeavours to ensurethat there are no personal data breaches.

In the unlikely event of a notifiable data breach, we will report to the ICO within 72 hours and follow the ICO procedure accordingly. All data breaches will be recorded and monitored by the DPO.

11. Links with other policies

This GDPR policy is linked to the following:

- Professional Code of Conduct for staff working in schools
- Child Protection Policy and Procedures
- Visitors Code of Conduct
- Governors Code of Conduct
- E-Safety and Acceptable Use Policy
- Freedom of Information Publication Scheme
- Telephone Calls, Mobile Phone, Camera and Video Usage Policy

This policy was approved by governors

At a meeting held on: 2.11.18 and reviewed for Federation November 2020

Review date: November 2022