Data Transfer Security Policy (GDPR compliant)

1. Aim and scope of the policy

The School stores a large volume of information both electronically and in paper form. This policy governs the procedures to protect this information and sets out how personal and sensitive data should be transferred around the School, and outside the School, in a secure and protected way.

This policy is applicable to anyone handling personal and sensitive data held in the school that may have a need to transfer this data including:

- Employees
- Workers
- Contractors
- Placement students
- Apprentices

Employees should read this policy in conjunction with the school's *Staff Use of ICT Policy*

2. The law

Data storage is regulated by the General Data Protection Regulation. Standards are set out in the Regulation and the current Data Protection Act.

3. Sensitive data

Sensitive data, for the purpose of this policy, includes data which contains:

- personal details about an individual (including those which are classed as special categories of data including data relating to health and race etc)
- confidential data about the School
- confidential data about goods, products or services
- confidential data about School customers and suppliers.

If anyone handling data is any doubt as to whether that data is or is not 'sensitive data', they must refer the matter to the Headteacher or their line manager.

4. Data transfers Considerations

Anyone handling personal or sensitive data must seek consent from the Headteacher or their line manager to authorise data transfer.

Data (sensitive or not) should only be transferred where it is strictly necessary for the effective running of the School. Accordingly, before any data transfers are requested, the necessity of the transfer should be considered in advance.

When dealing with third parties consider whether any data sharing agreements or contracts are in place that cover the transfer of that data. Check whether there are any stipulations in place regarding the method of transfer that should be used.

Check that you are not providing more information than is necessary for the identified purpose. For example, do not just send a whole document or spreadsheet when only one section or specific columns are required.

For all transfers of information containing personal or sensitive data, it is essential that you appropriately establish the identity and authorisation of the recipient.

5. Data Transfer Methods

Before choosing the method of transfer you must consider the following:

- The nature of the information, its sensitivity, confidentiality or possible value
- The size of the data being transferred
- The damage or distress that may be caused to individuals as a result of any loss during transfer
- The implications any loss would have for the school
- You must only send information that is necessary for the stated purpose, and any data not required should be redacted or removed completely (as appropriate) before transfer.

5.1 Data Transfer by Email

- Email communication should not be used to transfer unencrypted sensitive data which could contain personal information. Staff should be mindful that emails are not designed to attach and transfer large amounts of data. The School's email system does not support file attachments that exceeds the total of 25MB.
- Staff should consider an alternative secure method of transferring sensitive data wherever possible and practicable. If no suitable alternative is available then apply an extra level of security. This can be achieved by the use of encryption, applying a password to the sensitive data you wish to send. All passwords must be transferred using an alternative method of communication to the recipient (this includes post, telephone call to an agreed number, or by SMS text message).
- Email messages must contain clear instructions of the recipient's responsibilities and instructions on what to do if they are not the correct recipient.
- Information sent must, where practical, be enclosed in an attachment.
- Care must be taken as to what information is placed in the subject line of the email or in the accompanying message. Filename or subject line must not reveal the full contents of attachments or disclose any sensitive personal data.
- Emails must be sent from your email address, as provided by the school, to ensure the correct privacy and security information is displayed.

5.2 School Portal

For users who are required to copy or move data to removable media and the quantity of data to be transferred is too large then assistance should be sought from the school's ICT Support Team.

The Portal should not be accessed by staff through File Explorer without prior permission from the school's ICT Support Team.

Care must be taken when uploading data to the Portal, ensuring that filenames are appropriately named and stored in the correct locations. Sensitive data which is required to be uploaded to the Portal must not be stored in publicly accessible locations.

5.3. Uploading via School Secure

Any data being uploaded to School Secure must be carried out using their secure portal, following appropriate procedures.

5.4. Uploaded to online educational resources

Any data being transmitting to and from online educational resources must be encrypted, whether this is the use of a password protected document or encrypted zip file.

A Data Protection Impact Assessment must be carried out before transmitting data to and from online educational resources.

5.5 Removable storage devices (eg memory sticks, usb drives)

Any data being transferred by removable media (e.g. USB memory stick) should be encrypted. Encrypted portable storage devices must be password protected with a strong password. If the password itself must be conveyed to a third party, it must be transferred using an alternative method of communication to the recipient (this includes post, telephone call to an agreed number, or by SMS text message).

For users who are required to copy or move data to removable media and the quantity of data to be transferred is too large then assistance should be sought from the school's ICT Support Team.

Ownership of the removable media used must be established. The removable media must be returned to the owner on completion of the transfer and the transferred data must be securely erased from the storage device after use.

Clear instructions of the recipient's responsibilities and instructions on what to do if they are not the intended recipient must be given.

Any accompanying message or filename must not reveal the contents of the encrypted file.

The sender must check, at an appropriate time, that the transfer has been successful and obtain a receipt. An email confirming receipt is acceptable.

Report any issues to your line manager and in the case of missing or corrupt data to the Chief Privacy Officer or Data Protection Officer immediately (see contact details below).

5.6 Telephones and Mobile Phones

As phone calls may be monitored, overheard or intercepted (either deliberately or accidentally), care must be taken as follows:

- Personal data must not be transferred or discussed over the telephone unless you have confirmed the identity and authorisation of the recipient.
- When using answer phones do not leave sensitive or confidential messages, or include any personal data. Only provide a means of contact and wait for the recipient to speak to you personally.
- When listening to answer phone messages left for yourself, ensure you do not play them in open plan areas which risks others overhearing.

5.7 Data transfers by post/courier

Data transfers which occur via physical media such as memory cards or CDs must only be dispatched via secure post. The use of first or second class Royal Mail is not permitted; only Special Delivery or Recorded Delivery should be used. For non-Royal Mail services, a secure courier service must be used with a signature obtained upon delivery.

The recipient should be clearly stated on the parcel and the physical media must be securely packaged so that it does not break or crack.

The recipient should be advised in advance that the data is being sent so that they are aware when to expect the data. The recipient must confirm safe receipt as soon as the data arrives. The sender responsible for sending the data is responsible for confirming the data has arrived safely.

5.8 Hand Delivery and Collection

Hand delivery or collection of a document is also an approved method of transfer. When arranging for an individual to collect information, it should be established that they are who they say they are and seek an appropriate form of identification before handing over any documentation.

6. Lost or missing data

If an employee discovers that data has been lost or is missing, the employee is required to inform their line manager and Chief Privacy Officer immediately *who will refer the matter to the Headteacher and the School's Data Protection Officer. (see contact details below)*

The School's Breach Notification Policy will be followed.

The Headteacher must consider referring a matter to the police if it is found that unauthorised individuals have accessed sensitive data. Data which is held in the correct encrypted, compressed and/or password protected formats, which has been accessed by an unauthorised individual, has been accessed unlawfully.

7. Negligent data transfers

Employees who fail to comply with the requirements of this policy are likely to have their actions considered as gross misconduct, which may result in summary dismissal. Personal data breaches may result in exceptionally large fines for the School.

Employees must not be negligent when transferring sensitive data. Examples of negligence include failing to obtain authorisation, failing to ensure the data is appropriately encrypted, compressed and password-protected or using non-secure post services which are not tracked or insured.

8. Data Protection Officer

The School's appointed Data Protection Officer is the *Governance Manager* in respect of its data protection activities who can be contacted at Droitwich Spa High School and Sixth Form Centre, Briar Mill, Droitwich, WR9 0AA or by email at privacy@droitwichspahigh.worcs.sch.uk .

9. Chief Privacy Officer

The HR and Administration Manager is the School's appointed chief privacy officer in respect of its data protection activities who can be contacted at Droitwich Spa High School and Sixth Form Centre, Briar Mill, Droitwich, WR9 0AA or by email at privacy@droitwichspahigh.worcs.sch.uk

10. The School Website Privacy Page

The school's policies, privacy notices and forms are available on our web site at www.droitwichspahigh.worcs.sch.uk or by using the link below

https://public.droitwichspahigh.worcs.sch.uk/privacy