Rucstall Primary School
General Data Protection Regulation (GDPR) guidance for Governors

Data protection and data security is the responsibility of every member of the governing body.

Please read and comply with the following guidance:

Data Protection, Processing of Personal Data: Staff should always be clear about why they are processing data and should not process any personal information other than in accordance with the terms and conditions of the General Data Protection Regulations 2018. This means that you must have legitimate reasons for collecting and using (processing) the personal data; not use the data in ways that have unjustified adverse effects on the individuals concerned; handle people's personal data only in ways they would reasonably expect; make sure you do not do anything unlawful with the data; be open, transparent and honest about how you intend to use the data, i.e. by complying with the Governor Privacy Notice (which is attached to this guidance).

Please note:

1. Governors should be particularly careful with sensitive data

2. Governors must not process personal data for research/consultancy purposes unless the personal information is anonymised, or they have the written permission of the individual.

3. Individuals have a legal right to access their personal information therefore governors should be accurate and measured in what they write about students and members of staff.

4. Other than in the case of approved routine data transfers (e.g. returns to Government bodies/LA's) governors should not disclose personal information to external third parties without obtaining consent from the individual, or unless permitted to do so by law.

5. Email addresses are personal data. Do not send emails (e.g. to large numbers of recipients) showing the private email addresses of all the recipients. For confidentiality please blind copy the addressees and send the email to yourself when sending such emails.

6. All data should be organised in a sufficiently structured way so that the school can respond within seven days to a request for disclosure of personal information.

Data Security Reminders:

1. Keep secure all files containing personal data whether on paper or on computer.

2. All paper based personal information should be locked away at night.

3. Laptops, other portable equipment containing personal data, computer media like discs or memory sticks should also be locked up at night.

4. Email attachments (e.g. spreadsheets) containing personal data must be password protected and the password sent to the recipient in a separate email.

5. Take special care if taking other people's personal data off site.

6. If individuals disclose sensitive data/information, for instance about their health, ensure that it is stored securely and revealed only to those members of staff who need to know it.

7. Any personal data held on portable media must be encrypted/password protected.

Data Protection Subject Access Requests:

Governors have a right to access information that the school may hold on them. If a governor wants to see their personal data, they should speak to the Data Protection Officer. Most requests for personal data can be provided quickly and easily. If the employer is unable or unwilling to agree to the request, the governor could make a Subject Access Request. A subject access request should be in writing and include:

- full name, address and contact details
- details of the specific information required and any relevant dates.

Data Breaches:

All data breaches (accidental disclosures/losses of personal data) MUST be reported to your Data Protection Officer, Mrs S Tillman, as soon as the breach has been discovered so that appropriate measures can be taken to recover the data and limit any damage.

The school is obliged to report serious breaches to the Information Commissioner.

This statement was agreed and adopted by the Governing Body

on .....