23. Appendix 13 – Data Protection Overview Guidance for Staff

Data protection and data security is the responsibility of every member of staff who processes personal information. Please read and comply with the following guidance:

- 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 Schools Data Protection Policy.
- Staff may not process personal data without the individual's consent, unless there is a legitimate reason for doing so without consent.
- Parents/ Carers and Students have a legal right to access their personal information therefore staff should be accurate and measured in what they record.
- Other than in the case of approved routine data transfers (e.g. DofE/ National Pupil Database/ Onward Education Establishment) staff should not disclose personal information to external third parties without obtaining consent from the individual, or unless permitted to do so by law. If you are unsure, please contact the School Data Protection Officer.
- 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.
- Keep secure all files containing personal data whether on paper or on computer.
- Apply password protection to computers, screensavers and documents. Where possible keep your office door locked and your desk clear of personal data when you are absent
- All paper based personal information should be locked away at night.
- Laptops, other portable equipment containing personal data, computer should be locked up at night.
- Memory Sticks must not be used for transferring data
- Email attachments containing personal data must be by secure mail.
- 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.
- Confidential waste must always be shredded, and not put into a waste or recycling bin.

Data Breaches: All data breaches (accidental disclosures/losses of personal data) must be reported immediately to the School Data Protection Officer (at specialistredactionservice@gmail.com) and the Headteacher 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.