The Sandon School

Data Protection Policy
(including GDPR)

Last Adoption Date: March 2020

Next Review Date: Spring 2021

The Sandon School Data Protection Policy

Introduction

1. The Sandon School (The School) aims to ensure that all personal data it collects and processes about governors, staff, students, parents and other individuals who come into contact with the School is dealt with in accordance with Data Protection legislation. This includes General Data Protection Regulations (GDPR). This information regardless of whether it is in paper or electronic format is gathered in order to enable it to provide education and other associated functions. There is a legal requirement to collect and process information to ensure that the School complies with its statutory obligations.

2. The School is registered as a Data Controller with the Information Commissioner's Office (ICO) and is responsible for maintaining a current entry in the register of Data Controllers which is available on the ICO's website. The School will lawfully process as well as control data.

3. The School is required to issue a Privacy Notice to all governors, staff, students and/or parents and others for whom data is collected. This will summarise the information held on individuals, why it is held and the other parties it may be shared with.

4. Consent when appropriate is obtained directly. It will be explicit and unambiguous. When a child has the right to give consent this only relates to the control and processing of data and not the outcome of its use where the parents and school retain their rights of decision. Consent should be as easy to withdraw as to provide.

5. The School will comply with all current legislation and will undertake to inform, through communication and training, all staff of their responsibilities towards Data Protection and the associated policies and procedures of the School.

6. The Governing Board has responsibility for the School complying with legislation. The Headteacher is the Senior Information Risk Officer (SIRO) with overall responsibility The Business Manager will be the Data Protection Officer (DPO) and will be responsible for day to day matters including regular and systematic monitoring

7. This policy also includes the use of CCTV for which the School has internal procedures and impact assessments.

Purpose

8. This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with Data Protection legislation and other related law such as that relating to Human Rights. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. Our aim is to comply with all the rights of individuals with transparency and fairness. The School will ensure that sensitive information has enhanced protection.

What is Personal Information?

9. Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. I also applies to personal data held visually in photographs, video clips, CCTV, as sound recordings or biometric information.

Data Protection Principles

10 The Data Protection legislation establishes six enforceable principles that must be complied with. Personal data must be:

- processed fairly, lawfully and transparently;
- obtained only for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and where necessary, kept up to date;
- must not be kept for longer than is necessary for the purpose intended;
- processed in a manner that ensures the appropriate security of personal data.

General Statement

11 The School is committed to maintaining the above principles at all times. Therefore, the School will:

- Inform individuals why the information is being collected, when it is collected and with whom it is shared via the Schools' privacy notices.

- Process staff data for legal, personnel, administrative and management purposes in order to meet legal requirements as an employer.

- Keep all personal data stored so that it is accurate and not misleading. The School will remind governors, staff, parents and/or students and others annually to update the personal details held. However, everyone is requested to notify the School if any personal details change or if they become aware of any inaccuracies.

- Ensure in its procedure for the management of records that information is regularly reviewed and not retained for longer than is necessary. The School will comply with good practice and the records management policy of the Records Management Society.

- Ensure that when obsolete information is destroyed that it is done so appropriately and securely

- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft, unlawful and unauthorised disclosure, irrespective of the format in which it is recorded

- Share information with others only when it is legally appropriate to do so or an agreement is in place. This requires approval by the DPO.

- Ensure we have a procedure to process any requests for personal data as a 'Subject Access Request'; as prescribed by law.

- Ensure that Privacy Impact Statements are completed and approved where the processing is high risk to the rights of the data subjects

- Ensure that only those who have a lawful need to access personal data are able to do so. Staff and students must not access personal data which they have no right to view. Information will only be known to an appropriate audience

- Ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is being processed.

- Ensure that appropriate security controls are in place technically, physically and organisationally

- Not share any personal data with an individual or an organisation outside of the European Economic Area unless specific consent is obtained.

- Ensure our staff are aware of and understand our policies and procedures and are trained and informed of Data Protection legislation.

12. Where the content of telephone calls, emails, internet activity and video images are recorded, monitored and disclosed they must be in compliance with the regulators code of practices and school procedures. All data subjects must be aware of what is being recorded, why and in what circumstances it may be used

Complaints and Breaches

13. Complaints should follow the procedure set out in the Complaints Policy of the School. The Headteacher will consider issues as the SIRO If you are not happy with the decision please contact the ICO.

14. Staff will not store data on any device not under the control of, or permitted by the school. Breaches of this policy will be investigated and may result in disciplinary action. A serious breach may be considered gross misconduct and result in dismissal and/or legal action.

15. Governors, staff, students and/or parents and others must report all incidents involving breaches or potential breaches of this policy. They must follow the procedure of the School for investigation. The Headteacher as SIRO will notify the ICO within 72 hours of becoming aware of any major or critical breach and also notify any individual involved without delay

16. This policy will be well publicised. It will be reviewed at least annually. It was adopted using Chair's powers on 26 March 2020 and will be ratified formally by the Governing Board at the next Full Governors meeting.