Data Protection Policy

This document is a statement of the aims and principles of the School, for ensuring the confidentiality of sensitive information relating to staff, pupils, parents and governors.

Introduction
St John's and St Clement's School needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

Data Protection Principles
To do this, St John's and St Clement's School must comply with the Data Protection Principles which are set out in the Data Protection Act 1998. In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for that purpose.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.

St John's and St Clement's School and all staff or others who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the School has developed this Data Protection Policy.

Status of this Policy
This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the School from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

The Data Controller and the Designated Data Controllers
The School as a body corporate is the Data Controller under the 1998 Act, and the Governors are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day to day matters. The School has three Designated Data Controllers: They are the Headteacher, the School Business Manager and the Admin Officer.

Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the appropriate Designated Data Controller.

Responsibilities of Staff
All staff are responsible for:

- Checking that any information that they provide to the School in connection with their employment is accurate and up to date.
- Informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.

- If and when, as part of their responsibilities, staff collect information about other people (e.g. about a student's course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff set out in the School's Data Protection Code of Practice.

Data Security
All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.
Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe; or
- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
- If a copy is kept on removable storage media, that media must itself be password protected.

Rights to Access Information
All staff, parents and other users are entitled to:

- Know what information the School holds and processes about them or their child and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the School is doing to comply with its obligations under the 1998 Act.

This Policy document and the School's Data Protection Code of Practise address in particular the last three points above. To address the first point, the School will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the School holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should complete the Subject Access Request Form and submit it to the Designated Data Controller.
The School will make a charge of £10 on each occasion that access is requested, although the
School has discretion to waive this.

The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the 1998 Act.

Subject Consent
In many cases, the School can only process personal data with the consent of the individual. In some cases, if the data is sensitive, as defined in the 1998 Act, express consent must be obtained. Agreement to the School processing some specified classes of personal data is a condition of acceptance of employment for staff. This included information about previous criminal convictions.

Jobs will bring the applicants into contact with children. The School has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job. The School has a duty of care to all staff and students and must therefore make sure that employees and those who use School facilities do not pose a threat or danger to other users.

The School may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The School will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, or race. This may be to ensure that the School is a safe place for everyone, or to operate other School policies, such as the Sick Pay Policy or the Equal Opportunities Policy. Because this information is considered sensitive under the 1998 Act, staff (and students where appropriate) will be asked to give their express consent for the School to process this data. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

Publication of School Information

Certain items of information relating to School staff will be made available via searchable directories on the public Web site, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with the School.

Retention of Data

The School has a duty to retain some staff and student personal data for a period of time following their departure from the School, mainly for legal reasons, but also for other purposes such as being able to provide references or academic transcripts. Different categories of data will be retained for different periods of time.

Conclusion

Compliance with the 1998 Act is the responsibility of all members of the School. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution.

Note

We will need to undergo significant changes in May 2018 in order to fully satisfy the requirements of the GDPR.

Appendix 1 – Frequently Asked Questions

APPENDIX 1
FREQUENTLY ASKED QUESTIONS

1. What is "Data Protection"?

Data Protection within the UK refers to the Data Protection Act 1998 (DPA). This law exists to protect individuals about whom information (whether as an electronic records or in a databases or hard copy in a highly structured paper files) is held.

The DPA controls how this personal information can be processed and grants important rights to the individuals about whom personal data is collected.

The ways in which personal data can be used for electronic marketing communication (e.g. by email, fax, text message) is regulated by the Privacy & Electronic Communications (EC Directive) Regulations 2003.

2. What is personal data or personal information?

Personal data is any information which identifies – either directly or indirectly - a living individual. Data need not be extensive to be personal data – it could be as little as someone's name and contact details, even just a reference number like a staff ID, or a photograph. Provided it is capable of enabling an individual to be identified – it will be captured by the Act. Personal data is also sometimes referred to as personal information.

3. What is 'sensitive' personal data?

The DPA defines certain special categories of personal data as 'sensitive. These are certain types of information, historically seen as being the type of data that can disadvantage or harm individuals if improperly used - that require an extra level of protection

Any information relating to an individual in respect of:

a) racial or ethnic origin
b) political opinions
c) religious or similar beliefs
d) trade union membership
e) physical or mental health
f) sexual life
g) criminal convictions
h) proceedings against him/ her for an offence

The collection of sensitive personal data must be limited and obtained only with consent from the individual unless there are other specific legal grounds that would justify the collection of sensitive personal information without the consent from the individual.

Photographic images, like CCTV images may also be sensitive personal data where they have the ability to determine someone's ethnic background, religion or disabilities. This therefore needs to be judged on an individual basis.

Even if you are looking to collect limited video footage or photographs for an intranet site, you should contact the Privacy team who will be able to explain whether steps are required to be able to do this lawfully.

4. The term 'processing personal data' is often used, what does this mean?

Processing effectively means any action or operation performed on the personal information or data, for example:

- Obtaining
- Recording
- Holding
- Adapting
- Altering
- Retrieving
- Viewing
- Disclosing
- Transmitting
- Combining
- Archiving
- Erasing, deleting or destroying the information or data

5. What is the issue with international data transfers?

Data Protection laws says that personal data cannot be transferred outside the European Economic area (EEA) unless adequate protection and controls are in place.

6. Does personal data include opinions about individuals?

Yes - Opinions are classed as personal data, therefore you must be very careful when, for example, noting down comments about a person's behaviour; scribbling notes on an employee's file; or, making interview notes about a prospective employee.

The important points to bear in mind are:

(a) that the individual has a right to see any information held about him/ her, so you do not want to note down anything which is not factual or that you would not want to stand by should the individual ask to see, and if you are recording an opinion, make this clear in your notes/ on your system

(b) we should not be collecting information just because we can – ask yourself before noting anything down whether or not you really do need the information in order to carry out your job, or in order to ensure the purpose for which you are collecting the information is fulfilled

7. Is voicemail classed as personal data?

Yes – Where a voicemail identifies a living individual it falls within the definition of personal data.

8. Are CCTV cameras covered by the Act?

Yes – CCTV cameras and similar security devices are covered by the Act if they record and retain images about individuals. This means that images are subject to the rules on data protection in the same way as a personnel file would be.

9. What rights do individuals have to control the use of their personal data?

There are several rights granted to individuals but the key ones are:

(a) the right to prevent processing for direct marketing
An individual can insist at any time that an organisation stop processing their data for direct marketing purposes. Note – this is an absolute right and can be invoked regardless of circumstances and there are no exemptions that can be relied on to deny such a request.

(b) Right to access information
An individual can make an access request to any organisation to ask (i) if personal information about them is held by that organisation and (ii) to see all the information that is being processed.
The Data Protection Act gives access to electronically held information or data stored within a structured manual filing system but because Schools are subject to Freedom of Information which provides access to all information held by a public authority, individuals could potentially also have access to unstructured data – such as notes in a day book using this access right.

10. Who is responsible for ensuring that companies follow the legislation?

The Information Commissioner's Office (ICO) has responsibility for enforcing compliance with the UK Data Protection Act, 1998 and the Privacy and Electronic Communications Regulations 2003

11. Are there any guidelines laid down as to how the data needs to be stored/ held after its useful life?

Data Protection law says that personal data should not be kept once it has served its purpose. Whilst organisations often need to retain information for legal or commercial reasons for some length of time after the information ceases to be referred to regularly, processes should exist to establish time limits for retention and build in procedures to archive and delete information once these retention times have been met. This applies to systems /databases and paper records.