Protection of Pupil Data Policy (Whole School including EYFS)

Independent Day School for Boys and Girls

Our Lady of Sion School

Frequency of Review: 2 Years
Last review: July 2015
RR

No:23

Our Lady of Sion School

Policy on protection of pupil data

Policy statement

1 This policy is available to all members of staff and is available to parents, legal guardians and pupils on request.

2 The aim of the policy is to help us to comply with the Data Protection Act (the Act) when we process personal data about current, past or prospective pupils, their families and guardians.

3 This policy is aimed at all staff at the School including temporary staff, agency workers and volunteers. The policy explains the School's general approach to data protection, and provides practical guidance which will help to ensure that the School complies with the Act.

4 "Processing" may include creating, obtaining, recording, holding, disclosing, amending, destroying or otherwise using personal data (this expression is explained below).

5 We have appointed the Bursar as the School's Data Protection Officer (DPO) who will endeavour to ensure that all personal data is processed in compliance with this policy.

6 The School has registered its use of personal data with the Information Commissioner's Office and further details of the personal data the School holds, and how it is used, can be found in the School's register entry on the Information Commissioner's website at www.ico.gov.uk under registration number Z5791539. This website also contains further information about data protection.

The Data Protection Principles

7 The Act contains eight data protection principles which set out how organisations should handle personal data. They cover issues such as what information needs to be given to the individual, information security and using individuals' personal data in a fair way. The practical steps which the School should take to help comply with the 8 principles are explained in the sections below.

Meaning of "personal data"

8 "Personal data" means any information relating to an identified or identifiable individual. "Identifiable" includes one who can be identified indirectly, for example, by reference to an identification number or to one or more factors specific to physical, physiological, mental, economic, cultural or social identity.

9 Every school is required, as part of its operation, to process a wide range of personal data

which may include -

- Names, addresses, dates of birth and national insurance numbers.
- Bank details and other financial information.
- Academic, disciplinary, admissions and attendance records and references.
- Medical records.
- Examination scripts and marks.
- Photograph/s and CCTV images.
- Information about racial or ethnic origin and religious beliefs.

10 If a record containing personal data is held on a computer then it will be covered by the Act. This is the case regardless of how the information is held. For example personal data stored in an email, in a spreadsheet or on a Smartphone are all caught by the Act.

11 Records held in paper files only are sometimes not covered by the Act although there are so many exceptions to this rule that best practice is to treat all information about individuals as covered by the Act whether it is held in a paper file or held on computer.

Use of personal data

12 We may use personal data about a pupil, a parent or a legal or educational guardian (provided that such use is permissible under the Act) for the following purposes -

- Providing pupils and staff with a safe and secure environment, an education and pastoral care;
- Providing activities for pupils and parents - this includes school trips and activity clubs;
- Providing academic, examination and career references for pupils and staff;
- Protecting and promoting the interests and objectives of the School - this includes fundraising;
- Fulfilling the School's contractual and other legal obligations. For example, for the performance of our contract with parents;
- For the legitimate interests of the School or a third party (such as another school or an examining board).

13 School staff must not use personal data for any other purpose without the DPO's permission.

14 Staff should not use personal data for any purpose that is incompatible with the purpose for which it was originally acquired without obtaining the DPO's permission.

15 Staff will frequently disclose personal data. For example staff may routinely discuss a pupils' progress with parents. Similarly staff may discuss routine matters relating to pupils with colleagues.

16 All of this is allowed by the Act but staff should not disclose personal data in circumstances which might be considered unusual, or where the personal data includes sensitive personal data (see below), without permission from the DPO. Staff should always speak to the DPO if in doubt about whether a disclosure of personal data is permissible.

17 Staff must not transfer personal data outside the European Economic Area (EEA) without the individual's permission unless the School is satisfied that the individual's rights under the Act will be adequately protected and the transfer has been approved by the DPO. This applies even if the transfer is to a pupil's parents or guardians living outside the EEA.

Sensitive personal data

18 There are extra obligations in relation to sensitive personal data held by the School. Sensitive personal data is information about an individual's racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life and information relating to actual or alleged criminal activity.

19 Staff should not handle sensitive personal data without discussing with the DPO first.

Rights of access to data

20 Individuals have a right of access to their personal data unless an exemption applies (see below). An individual wishing to access their personal data should put their request in writing to the DPO. We will respond to a request for access to records within forty days of receiving the request (provided that we have all the information which we need in order to deal with the request).

21 The School is entitled to charge an administration fee (usually £10) for responding to a request.

Exemptions from the right of access

22 The Act provides that certain data is exempt from the right of access, including -

- Information which identifies other individuals
- Information which we reasonably believe is likely to cause damage or distress
- Data used in connection with legal proceedings
- Examination scripts written by a pupil
- Data that does not concern a living individual

- Data that is held in certain unstructured filing systems
- Data that may be evidence in criminal proceedings

23 Please note that the above exemptions do not apply in all cases. For example, sometimes the School may be required to disclose personal data even where it identifies other individuals.

24 We will also treat as confidential any reference in our possession which has been prepared or given to UCAS and any reference for current or prospective education, training or employment of a pupil. We acknowledge that an individual may have a right of access to a reference which we receive about them from another source. Such reference will only be disclosed, however, if -

- Disclosure will not identify the source of the reference; or
- The referee has given consent; or
- Disclosure is reasonable in all the circumstances.

Who can exercise the rights

25 Rights under the Act belong to the individual to whom the personal data relates.

26 We will only grant a pupil direct access to their personal data if we reasonably believe that the pupil understands the nature of the request. We would usually expect a pupil to understand the nature of a request from the age of twelve.

Requests from third parties

27 We will normally disclose such data as is necessary to third parties for the following purposes -

- To give a confidential reference relating to a pupil to any educational institution which it is proposed that the pupil may attend, or to a prospective employer;
- To give information relating to outstanding fees or payment history to any educational institution which it is proposed that the pupil may attend;
- To publish the results of public examinations or other achievements of pupils at the School;
- To publish non-portrait-style photographs or images of pupils who are not identified by name in our prospectus or promotional video or on our website;
- To disclose details of a pupil's medical condition, allergies or disability, where it is in the pupil's interests that we do so, for example, for medical advice, insurance purposes or to members of staff supervising sports and games or to organisers of school trips.

28 In most other cases, we will not generally disclose personal data to third parties unless the individual has given consent or one of the specific exemptions under the Act applies. If we receive a disclosure request from a third party we will take all reasonable steps to verify the

identity of the third party before making any disclosure.

29 A parent, or a pupil aged 12 years plus, who wishes to limit or object to the pupil's image being used in the School's promotional material should please notify the DPO in writing. In the absence of such notification, we will, from time-to-time, make use of personal data relating to pupils, their parents or guardians in the following ways –

- In our prospectus, video, website or other promotional literature or materials; we will not, however, publish a portrait-style photograph or the pupil's name for marketing purposes without the express agreement of a parent or a pupil aged 12 years or more.

- To compile and maintain our register of current or former pupils or any necessary list of pupils representing the School as a member of a team or on a school trip.

- To give information relating to the fundraising activities of the School and initiatives considered beneficial to members of the School community.

- To maintain contact with former members of the School and their association and to inform them of events and activities.

30 Only staff with the appropriate authorisation from the School may access personal data. Personal data shall not be disclosed to anyone who does not have the appropriate authority to receive such information, irrespective of their seniority within the School or their relationship to the subject of the personal data, unless they need to know it for a legitimate purpose. Examples:

- The School Nurse may disclose details of a lunchtime supervisor's allergy to bee stings to colleagues so that they will know how to respond, but more private health matters must be kept confidential; and

- Personal contact details for a member of staff (e.g. their home address and telephone number, and their private mobile telephone number and e-mail address) shall not be disclosed to parents, pupils or other members of staff unless the member of staff has given their permission.

Handling personal data in general

31 The School must process personal data in a way that is fair to individuals. Compliance with this policy is likely to mean that the processing is fair in most cases. However, the concept of fairness can be quite difficult to define and staff should inform the DPO if they feel that any of the processing of personal data appears to be unfair to any individual in any way even if the processing appears to comply with the letter of this policy.

32 The School must only keep personal data for as long as is reasonably necessary but staff should not delete records containing personal data without authorisation. Staff should consult with the DPO for guidelines about how long to retain different categories of personal data.

33 Staff should ensure that personal data is complete and kept up-to-date. For example, if a parent notifies a member of staff that their contact details have changed, the member of staff should inform the DPO so that the School's central record can be updated.

34 The School must ensure that it has sufficient personal data. For example a teacher writing a report about a pupil should ensure that he/she has all the pupil's relevant records to hand.

35 The School must not process personal data in a way that is excessive or unnecessary. For example, should 8 pupils out of a class of 20 attend a field trip, the member of staff should only take records (such as information about allergies and parent contact details) of those eight.

Informing the individual

36 If the School obtains personal data (whether from the individual or from a third party) it will need to explain to the individual what the personal data will be used for. This is sometimes called a Privacy Notice.

37 The Privacy Notice must explain what information will be collected, what it will be used for, which third parties (if any) it will be shared with and anything else which might be relevant.

38 Staff are not expected to routinely provide pupils, parents and others with a Privacy Notice as this should have already been provided.

39 Having said this, staff should inform the DPO if they suspect that the School is using personal data in a way which might not be covered by an existing Privacy Notice. This may be the case where, for example, staff are aware that the School is collecting medical, information about pupils without telling the pupils what that information will be used for.

Data security

40 A member of staff who deliberately or recklessly discloses personal data held by the School without proper authority is guilty of a criminal offence and gross misconduct. This could result in summary dismissal.

41 Staff must do all that they can to ensure that personal data is not lost or damaged, or accessed or used without proper authority. In particular:

- paper records which include confidential information shall be kept in a cabinet or office which is kept locked when unattended;
- computers must be kept locked when not in use;
- the School uses a range of measures to protect personal data stored on computers, including file encryption, anti-virus and security software, user passwords, audit trails and back-up systems. These must be used in all cases. Passwords must be at least 8 characters in length, be difficult to guess and should be changed frequently;
- staff must not remove personal data from the School's premises unless it is stored in an encrypted form on a password protected computer or memory device. Further information is available from the [Head of IT];
- staff must not remove sensitive personal data from the School's premises without permission from the DPO;

- staff must not use their own computers or their own email accounts when handling personal data relating to the School. For example, they must not send School related emails to their private email account;

- staff must not allow unauthorised access to School computers or computers containing School related personal data. For example, staff should not allow pupils or their friends and family access to their work computers or work emails;

- permission should be sought from the DPO before publishing anything containing personal data (for example, uploading photographs of a school trip to the School's website).

- staff must not use or leave portable electronic devices where there is a significant risk that they may be viewed or taken by unauthorised persons: they should not be viewed in public, and they must never be left in view in a car, where the risk of theft is greatly increased.

42 Any record containing personal data should be securely destroyed unless the information contained in the record is not very sensitive.

43 When disposing of computer records containing personal data it is important to make sure that the record is permanently deleted. It is not sufficient just to move the file into the recycle bin. Specialist software should be used to permanently delete the computer record. Further information is available from the IT Network Manager.

Authorised by: Chairman of Governors Date: