k

DATA PROTECTION POLICY

General Statement of the School's Duties

Beechwood Sacred Heart School is required to process relevant personal data regarding employees and pupils as part of its operation and shall take all reasonable steps to do so in accordance with this policy.

This Policy

This policy is intended to provide information about how the school will use (or "process") personal data about individuals including current, past and prospective pupils; and their parents, carers or guardians (referred to in this policy as "parents").
It applies in addition to the school's terms and conditions, and any other information the school may provide about a particular use of personal data, including e.g. the school's policy on taking, storing and using images of children.
Anyone who works for, or acts on behalf of, the school (including staff, volunteers, governors and service providers) should also be aware of and comply with the school's data protection policy.

Data Protection Controller

Beechwood Sacred Heart School has appointed the Bursar as the Data Protection Officer (DPO) who will endeavour to ensure that all personal data is processed in compliance with this policy and the Principles of the Data Protection Act 1998 and has been informed by the guidance given in the *Caldicott Principles* (1997) and more recently, by Fiona Caldicott (March 2013) *Information: To share or not to share? The Information Governance Review published by the Department of Health.*

The Principles

Beechwood Sacred Heart School shall so far as is reasonably practicable comply with Data Protection Principles (the Principles) contained in the Data Protection Act to ensure all data is:

- Fairly and lawfully processed
- Processed for a lawful purpose
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection.

Personal Data

Personal data covers both facts and opinions about an individual. It includes information necessary for employment such as the employee's or pupil's name and address and details for payment of salary.

Types of Personal Data Processed by the School

The school may process a wide range of personal data about individuals including current, past and prospective pupils and their parents as part of its operation, including by way of example:
names, addresses, telephone numbers, e-mail addresses and other contact details; car details (about those who use our car parking facilities); bank details and other financial information, e.g. about parents who pay fees to the school; past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks; where appropriate, information about individuals' health, and contact details for their next of kin; references given or received by the school about pupils, and information provided by previous educational establishments and/or other professionals or organisations working with pupils; and images of pupils (and occasionally other individuals) engaging in school activities, and images captured by the school's CCTV system (in accordance with the school's policy on taking, storing and using images of children).
Generally, the school receives personal data from the individual directly (or, in the case of pupils, from parents). However in some cases personal data may be supplied by third parties (for example another school, or other professionals or authorities working with that individual), or collected from publicly available resources.
The school may, from time to time, need to process "sensitive personal data" regarding individuals. Sensitive personal data includes information about an individual's physical or mental health, race or ethnic origin, political or religious beliefs, sex life, trade union membership or criminal records and proceedings. Sensitive personal data is entitled to special protection under the Act, and will only be processed by the school with the explicit consent of the appropriate individual, or as otherwise permitted by the Act.

Use of Personal Data by the School

The school will use (and where appropriate share with third parties) personal data about individuals for a number of purposes as part of its operations, including as follows:
For the purposes of pupil selection and to confirm the identity of prospective pupils and their parents; To provide education services (including SEN), career services, and extra-curricular activities to pupils; monitoring pupils' progress and educational needs; and maintaining relationships with alumni and the school community;
For the purposes of management planning and forecasting, research and statistical analysis, and to enable the relevant authorities to monitor the school's performance;
To give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil attended or where it is proposed they attend; and to provide references to potential employers of past pupils;
To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the school;
To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;

To monitor use of the school's IT and communications systems in accordance with the school's IT Acceptable Use policy;
To make use of photographic images of pupils in school publications, on the school website and (where appropriate) on the school's social media channels in accordance with the school's policy on taking, storing and using images of children;
For security purposes, and for regulatory and legal purposes (for example child protection and health and safety) and to comply with its legal obligations; and where otherwise reasonably necessary for the school's purposes, including to obtain appropriate professional advice and insurance for the school.

Processing of Personal Data
An employee or parent's consent may be required for the processing of personal data unless processing is necessary for the performance of the contract of employment. Any information which falls under the definition of personal data, and is not otherwise exempt, will remain confidential and will only be disclosed to third parties with the consent of the employees or parents.

Sensitive Personal Data
Beechwood Sacred Heart School may, from time to time, be required to process sensitive personal data regarding an employee or pupil. Sensitive personal data includes medical information and data relating to religion, race, trade union membership and criminal records and proceedings. Where sensitive personal data is processed by the School, the explicit consent of the employee or parent will generally be required in writing.

Keeping in touch and supporting the School

The school will use the contact details of parents, alumni and other members of the school community to keep them updated about the activities of the school, including by sending updates and newsletters, by email and by post. Unless the relevant individual objects, the school may also:
Share personal data about parents and/or alumni, as appropriate, with organisations set up to help establish and maintain relationships with the school community, such as the Friends of Beechwood.
Should parents wish to limit or object to any such use, or would like further information about them, please contact the DPO in writing

Rights of Access to Personal Data ("Subject Access Request")
Employees and parents have the right of access to information held by Beechwood Sacred Heart School. Any employee or parent wishing to access their data should put their request in writing to the Headmaster. The school will endeavour to respond to any such written requests (known as "subject access requests") as soon as is reasonably practicable and in any event, within 40 days for access to records and 21 days to provide a reply to an access to information request. The information will be imparted to the applicant as soon as is reasonably possible after it has come to the school's attention. The school may charge an administration fee of up to £10 for providing this information. You should be aware that certain data is exempt from the right of access under the Act. This may include information which identifies other individuals, or information which is subject to legal professional privilege. The school is also not required to disclose any pupil examination scripts (though examiners' comments may fall to be disclosed), nor any reference given by the school for the purposes of the education, training or employment of any individual.
Pupils can make subject access requests for their own personal data, provided that, in the reasonable opinion of the school, they have sufficient maturity to understand the request they are making.

Pupils aged 12 or over are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested. All subject access requests from pupils will therefore be considered on a case by case basis.
A person with parental responsibility will generally be expected to make a subject access request on behalf of younger pupils. A pupil of any age may ask a parent or other representative to make a subject access request on his/her behalf.

Whose Rights

The rights under the Act belong to the individual to whom the data relates. However, the school will in most cases rely on parental consent to process personal data relating to pupils (if consent is required under the Act) unless, given the nature of the processing in question, and the pupil's age and understanding, it is more appropriate to rely on the pupil's consent. Parents should be aware that in such situations they may not be consulted.
In general, the school will assume that pupils consent to disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare, unless, in the school's opinion, there is a good reason to do otherwise.
However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the school will maintain confidentiality unless, in the school's opinion, there is a good reason to do otherwise; for example where the school believes disclosure will be in the best interests of the pupil or other pupils.
Pupils are required to respect the personal data and privacy of others, and to comply with the school's relevant policies, e.g. IT Acceptable Use policy and the Beechwood Code.

Data Accuracy and Security

The school will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals must notify the DPO of any changes to information held about them.
An individual has the right to request that inaccurate information about them is erased or corrected (subject to certain exemptions and limitations under the Act) and may do so by contacting the DPO in writing.
The school will take appropriate technical and organisational steps to ensure the security of personal data about individuals. All staff will be made aware of this policy and their duties under the Act.

Storage and transmission of Sensitive Personal Data
All personal data must be stored securely. For hard-copies of documents this would mean storage in a secure (lockable) cupboard, cabinet or draw.

Files containing sensitive personal information on computers must be encrypted with a password. Beechwood Sacred Heart School computers are encrypted with passwords.

Sensitive personal data transmitted by a flash-drive must be password protected. It is recommend that for information stored and utilised using this method, only flash-drives given by the School should be used.

Queries and Complaints

Any comments or queries on this policy should be directed to the DPO. If an individual believes that the school has not complied with this policy or acted otherwise than in accordance with the Act, they should utilise the school complaints procedure and should also notify the DPO.

Appendix A

Guidance & Best Practice for all staff on the application of the Data Protection Act

Professional standards and good practice

Below contains the revised Caldicott Principles (March 2013) which govern data protection within the NHS. They are deemed to be best practice for any organisation that holds personal data.

1. Justify the purpose(s)

2. Do not use personal confidential data unless it is absolutely necessary

3. Use the minimum necessary personal confidential data

4. Access to personal confidential data should be on a strict need-to-know basis

5. Everyone with access to personal confidential data should be aware of their responsibilities

6. Comply with the law

7. The duty to share information can be as important as the duty to protect pupil/teacher/parent confidentiality

Personal information

Our records may contain the following types of personal information:

- Identification details: Names, addresses, National Insurance numbers, etc.
- Personal characteristics: Age, sex, date of birth, physical description, habits, facts about the person.
- Family circumstances: Marital details, family details, household members, social contacts.
- Social circumstances: Accommodation details, leisure activities, lifestyle.
- Financial details: Income, expenditure (School related), bank details, allowances, benefits and pensions.
- Other information: Employment details; qualifications /assessments; details of complaints, allegations, accidents or incidents.

Our records may contain sensitive, personal information which might include the following:

- racial or ethnic origin;
- religious beliefs or beliefs of a similar nature;
- trade union membership;
- physical or mental health or condition;
- commission or alleged commission of any offence; or in relation to proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

Extra care must and would necessarily be taken when processing sensitive personal data.

Before recording or otherwise processing sensitive personal information, you/we must be satisfied that it can meet one or more of the conditions specified in the DPA which allow the processing to take place.

Management of personal information
All staff must ensure they consider the following when they process personal information:

- Its Relevance: Personal information obtained, used and shared must be relevant to Beechwood Sacred Heart;
- Its Accuracy: Inaccurate information is dangerous as well as useless;
- Its Security: Keep it safe. Watch what you leave lying around or on the photocopier. Be careful when emailing data;
- Keeping data: Keep it safe. Keep it for length of time that is appropriate. Dispose of it securely and safely.

Appendix B

Guidance for staff in handling and storing information

- Papers, files, hard drives, CDs, flash-drives or other media that contain personal data must be guarded at all times, kept securely and locked away when the offices are vacated.
- The keys to cabinets should be kept safe.
- Where possible, documents should be kept in parts of the building protected by an alarm system.
- Staff should ensure that personal information is not provided to any unauthorised person no matter who they are – even the police or social services must obtain authorisation.
- Documents containing personal information must be posted in sealed envelopes which are properly addressed, clearly marked e.g. 'private and confidential' and sent via recorded delivery at all times.
- All sensitive personal information must be encrypted.
- All non-electronic material which contains personal data and has been authorised for disposal must be shredded/incinerated or disposed of using a regulated, professional data removal company.
- The School Office must ensure that documents, including those on computer screens, are not visible to those who do not have the right to view them.

Telephone enquiries

- Personal data or other confidential information must not be provided to telephone callers unless the staff member has satisfied themselves as to the identity of the caller and is certain that it is necessary to provide the information.
- If a staff member cannot confirm the caller's identity or has reason to doubt the identification provided they must make additional checks and telephone the caller back, using a telephone number from our existing records rather than one provided by the caller.
- If an employee has any doubts about whether to disclose personal data they should ask the caller to submit a written request for the information and seek guidance from their line manager or another appropriate senior manager.

Electronic records (including e-mails)

- Emails are not a secure method of communication.
- They can go astray, be intercepted or be forwarded on to a number of people who are not entitled to see them within minutes.
- They can also be addressed incorrectly - people could type in an address incorrectly or select a name from the suggestions which appear when typing into the 'To' field and accidentally send the email to the wrong recipient.
- This also applies to emails meant for internal recipients; they can easily be sent to the wrong recipient or even an external recipient by mistake. If the email is not encrypted, the personal information in it will be disclosed to people who are not entitled to see it.
- A disclaimer needs to be included within your address cards/signatures on all emails which are also being sent out. School emails will all have this disclaimer at the bottom:

Please check yours has.

- Check, check and check again that you are sending your email to the intended recipient
- Remember that emails are the same as any other type of document or official communication.
- Do not retain them if there is no business or legislative need for the information they contain.
- Remember that anything you write in an email could be disclosed to the public under FOI (Freedom of Information) or EIRs (Environmental Information Request) or disclosed to an individual if it is about that person.
- Anything you write in an email could be forwarded on to anyone once you have sent it; remember they are not secure or private! Ensure you password protect and encrypt any documents being sent via an email if containing personal information.
- Computer systems must be password-protected. Passwords must not be written down or disclosed and employees must not allow colleagues to use their individual usernames and passwords.

All staff must log out of their computer fully and ensure the monitor is switched off before leaving the office to go home. Laptops must be removed from desks and locked away in a secure place. (See the *ICT Acceptable Use Policy*)

Audio-visual records

Photographs of individuals should not be used unless you have obtained consent from them (or in the case of young people, from their parents or guardians). Policy and procedure about the use of

cameras, e.g., for EYFS staff are found in the ICT *Acceptable Use Policy* and the *Safeguarding Policy.)*

Glossary:

Data: Qualitative or quantitative statements or numbers that are (or are assumed to be) factual. Data may be raw or primary data (e.g. direct from measurement), or derivative of primary data.

Data breach: Any failure to meet the requirements of the Data Protection Act, unlawful disclosure or misuse of personal confidential data and an inappropriate invasion of people's privacy.

Data controller: A person (individual or organisation) who determines the purposes for which and the manner in which any personal confidential data are or will be processed. Data controllers must ensure that any processing of personal data for which they are responsible complies with the Act119.

Processing Data: Processing data' refers to every act carried out in relation to the data, from recording it through to viewing it, altering it and communicating it.

(September 2018)