DATA PROTECTION POLICY

GENERAL OVERVIEW

This policy is for Brighton College and its subsidiaries (together "the school").

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. ICT Acceptable Use Policy, Security Policy, Mobile Devices Policy.

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 for staff, which also provides further information about how personal data about those individuals will be used.

Pupils and parents are required to respect the personal data and privacy of others and comply with the school's policies relating to pupils and parents and the parent handbook.

RESPONSIBILITY FOR DATA PROTECTION

In accordance with the Data Protection Act 1998 ('the Act'), the school has notified the Information Commissioner's Office ("ICO") of its processing activities. The school's ICO registration number is Z1718351 and its registered address is Brighton College, Eastern Road, Brighton, BN2 0AL.

The School has appointed the Bursar as Data Protection Officer ("DPO") who will endeavour to ensure that all personal data is processed in compliance with this policy and the Act.

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 (but not limited to):

- names, addresses, telephone numbers, e-mail addresses and other contact details;
- car details (about those who use our car parking facilities or who cause disruption to other road users adjacent to the school or of parents who are aggressive with staff members if for example, parking is not or is not made available);
- 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;

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 generally be processed by the school with the explicit consent of the appropriate individual, or as otherwise permitted by the Act, although the school may consider real or potential safeguarding, health and safety and other legal requirements of more importance than compliance with the Act in areas where there is potential or real conflict.

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 ICT: acceptable use policy;
- To make use of photographic images of pupils, volunteers and staff in school publications, on the school website and on the school's social media channels in accordance with the school's policies on taking, storing and using images of children;
- For security purposes (including the capture and retention of images on the school's CCTV cameras), 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.

KEEPING IN TOUCH AND SUPPORTING THE SCHOOL

The school will use the contact details of pupils, 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;
- Contact parents and/or alumni (including via any external organisations used for the purpose) by post and email in order to promote and raise funds for the school and, where appropriate, other worthy causes;
- Collect information from publicly available sources about parents' and former pupils' occupation and activities, in order to maximise the school's fundraising potential.

Should you 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")

Individuals have the right under the Act to access to personal data about them held by the school, subject to certain exemptions and limitations set out in the Act. Any individual wishing to access their personal data should put their request in writing to the DPO.

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 statutory time-limits. 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, information which the school reasonably believes is likely to cause damage or distress, or information which is subject to legal professional privilege. The school is also not required to disclose any pupil examination scripts, nor any reference given by the school for the purposes of the actual or prospective 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.

An individual may have the right of access to a reference relating to them received by the school. However, such a reference will only be disclosed if such disclosure will not identify the source of the reference or where the referee has given their consent or where the disclosure is reasonable in the opinion of the school in all the circumstances.

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.

The school will only grant a pupil direct access to their personal data if in the school's reasonable belief the pupil understands the nature of the request.

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 or where disclosure is required by law.

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 school rules.

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.

QUERIES AND COMPLAINTS

If an individual believes that the school has not complied with this policy or acted otherwise than in accordance with the Act, they can utilise the school complaints / grievance procedure and if so, they should also notify the DPO.

Any comments or queries on this policy should be directed to the DPO in writing to: The Bursar, Brighton College, Eastern Road, Brighton, BN2 0AL.

PTW 07 December 2016

APPENDIX: Staff guidelines for the handling of personal data

A. INTRODUCTION

Data Protection Act (1998)

The Data Protection Act (1998) ("the Act") provides a framework to regulate the collection and use of personal information about living, identifiable individuals. These guidelines are provided to ensure that all staff, governors, volunteers and service providers are aware of their obligations in relation to handling personal data for doing so, whether the information is about staff, parents or students.

Personal Data

Any information relating to a living person and which can be identified as referring to him or her is included, whatever the format – electronic, paper, film, tape, text, still and moving images.

Sensitive personal data

Sensitive personal data has a very specific meaning in terms of the Act: information relating to race political opinion; religious belief; trade union membership; physical or mental health; sexuality; and any criminal history.

B. GUIDELINES

Collection and use of personal data

Only information which is really necessary should be collected. Nothing should be either requested or recorded on the grounds that 'it might come in useful'. Neither should it be used for purposes inconsistent with those specified in the College's Data Protection Policy.

Extra care should be taken in the handling and storage of sensitive personal data as defined in the introduction.

Storage

Precautions should be taken to prevent any unauthorised access to personal data. Any information relating to named individuals should be handled and stored securely, so:

- Desks or filing cabinets should be locked.
- Computers should be password protected.
- Papers should not be left out on desks or tables.
- Information on computer screens should not be accessible/ visible to other than authorised users.
- 'Sensitive' data should be secure and subject to very limited access.

Personal data should not be removed from the College or stored elsewhere unless it is logged and authorised. Off-site security must conform to College Standards as outlined above.

To minimise the risk of personal data being mishandled, it is recommended that information be held in one file wherever possible, rather than being dispersed or duplicated in several places. For example, material concerning current students should be held on file in the school office with the maintenance of separate files by tutors being avoided as far as is practicable and possible.

Data should not be held indefinitely unless this conflicts with requirements of other legislation considered to take primacy – the Goddard Enquiry and subsequent rulings means this requirement is changing regularly and for the most current information, the Archivist and/or Assistant Bursar should be referred to.

Disclosure
No information should be given to any third party without permission of the member of staff or student. This includes parents or other relations, partners, friends, colleagues, fellow pupils. Further details, including circumstances where disclosure is permitted, are outlined in other sections of this guidance and the Data Protection Policy.

In particular, it should be noted that the police have certain powers under the Act to access personal information which we hold. This is not an automatic right, however, and must be in relation to investigation/detection of a crime and/or apprehension of an offender. Extreme care must be taken to establish the identity of the caller and no information should be divulged without an official written communication showing crime number and the name, rank and badge number of the investigating officer. In case of uncertainty, please refer the matter to the Bursar.

Providing references
When supplying a reference, it should be assumed that the subject will have the right to read it. Although access to personal references does not have to be provided by the writer, in most cases the subject will be able to request a copy through the recipient. Information should be factual and verifiable with unsubstantiated opinion being avoided.

E mail to parents
When sending e mails to the parents of more than one pupil or groups of parents (e.g. to parents of pupils going on a trip) please be aware that you may be sharing personal information without permission. Please ensure that you send the e mail to yourself and blind copy (bcc) in the group of parents.

Disposal
Records should be disposed of securely through shredding or through a third party with appropriate accreditation for secure disposal to ensure no accidental disclosure to any third parties. Please contact the Head of Cleaning should you wish to ensure that the container you are disposing of information in is sufficiently secure for these purposes.