ETON COLLEGE
SCHOOL POLICY

DATA PROTECTION AND FAIR PROCESSING NOTICE

REVIEW DATE: MICHAELMAS 2017

1. ABOUT THIS POLICY

1.1 The College needs to process personal data about its current, prospective and former pupils and their parents, its current, prospective and former staff, its suppliers/ contractors, its current and prospective supporters and other individuals connected to the College, as part of its everyday operations. The College will process such personal data in accordance with the Data Protection Act 1998 ("the DPA").

1.2 The College is the data controller of this personal data under the DPA and has notified its use of personal data with the Information Commissioner's Office (ICO) under registration number Z5950637. The College is committed to compliance with the DPA and takes seriously the responsibility of handling personal information.

1.3 This Policy sets out the basis on which the College processes personal data. Please read the Policy carefully to understand the College's practices regarding personal data and how it will be treated.

2. DATA PROTECTION OFFICER

2.1 The College has appointed the Clerk and Legal Advisor to the Provost and Fellows as its Data Protection Officer.

2.2 The Data Protection Officer is responsible for:

- the College's notification as a data controller with the ICO and the notification (where required) of the College's subsidiary companies or trusts as data controllers;
- endeavouring to ensure that personal data is processed by the College in compliance with this Policy and all applicable data protection laws, including the data protection principles contained in the DPA ("the Data Protection Principles");
- arranging appropriate training for members of the College's staff who are responsible for processing personal data;
- being available to assist individuals about whom personal data is processed by the College ("data subjects") on issues relating to data protection practices and the DPA; and
- the enforcement, monitoring and review of this Policy.

3. THE DATA PROTECTION PRINCIPLES

The Data Protection Principles require the College to ensure all personal data is:

- fairly and lawfully processed;
- processed for one or more lawful purposes;
- adequate, relevant and not excessive;
- accurate and, where necessary, kept up to date;
- not kept for longer than necessary;
- processed in accordance with the data subject's rights;

- protected by appropriate security measures; and
- not transferred to countries outside the EEA without adequate protection.

4. PERSONAL DATA PROCESSED BY THE COLLEGE

4.1 Personal data processed by the College can take different forms – it may be factual information (such as names, ages and home addresses), expressions of opinion about a data subject, images of or including data subjects or other recorded information which identifies or relates to a living individual.

4.2 Personal data processed by the College includes a data subject's contact details and: (for staff and contractors) additional information required for their employment or appointment including images, audio and video recordings and biometric data; (for pupils) admissions, academic, disciplinary and other education related records, information about special educational needs, references, examination scripts and marks, images, audio and video recordings and biometric data; (for parents and/ or guardians) employment details, family circumstances and financial information.

4.3 Sensitive personal data processed by the College about an individual includes data concerning their sexual life, racial or ethnic origin, religious beliefs, criminal records and proceedings, trade union membership and relevant medical information (including details of a data subject's physical or mental health).

4.4 The College collects the personal data it processes directly from the data subject (or in the case of a pupil, his parents or guardians) and from third parties (for example, referees, previous schools, NCTL and the Disclosure and Barring Service).

5. PURPOSES FOR WHICH PERSONAL DATA MAY BE PROCESSED

Personal data (including sensitive personal data, where appropriate) is processed by the College in accordance with the Data Protection Act for the following purposes:

- **The provision of education** including the registration of prospective pupils and administration of the admissions process; administration of the school curriculum and timetable; administration of pupils' entries to public examinations, reporting upon and publishing the results; providing references for pupils (including after a pupil has left); and preparation of information for inspections by the Independent Schools Inspectorate.
- **The provision of educational support and ancillary services** including the provision of pastoral care, welfare, health care services and maintenance of discipline; provision of careers and library services; administration of sports fixtures and teams, school trips; boarding house administration; the administration of the School's Acceptable Use Agreement by monitoring pupils' email communications and internet use.
- **The research into and development of effective teaching and learning methods and best practice** at the College's Tony Little Centre for Innovation and Research in Learning including the provision of professional development to its staff and staff of schools associated with the College (such as the London Academy of Excellence, Holyport College and the schools within the Independent State School Partnership of which the College is a member).
- **The general administration of the College** including the compilation of pupil records; the administration of invoices, fees and accounts; the management of the College's

property; the management of security and safety arrangements (including the use of CCTV); the administration and implementation of the College's policies; and other reasonable purposes related to the College's operations.

- **The protection and promotion of the College's legitimate interests and objectives** including the publication of its own websites, its internal communication system and virtual learning environment, the prospectus, *Fixtures* and other publications; fund-raising for the College's charitable purposes; the maintenance of a historic archive; and communicating with the body of current and former pupils and/or their parents or guardians.
- **The administration of its staff, agents and suppliers** including the recruitment of staff/ engagement of contractors (including compliance with DBS procedures); administration of payroll, pensions and sick leave and the maintenance of appropriate human resources records for current and former staff; and providing references.
- **The fulfilment of the College's contractual and other legal obligations**

6. MEANS OF PROCESSING AND TRANSFERS OF PERSONAL DATA

6.1 The College will only process personal data for the purpose(s) for which it was originally acquired or which have subsequently been notified to the data subject(s) and will not process it for any other purpose without the data subject's permission, unless it is permitted to do so under the DPA. The College may communicate with data subjects for the purposes set out above by post, email and SMS.

6.2 Personal data shall only be disclosed to those members of the College's staff, agents and suppliers who need to access the personal data to process it for the purpose(s) for which it was acquired. The College adopts appropriate security measures to ensure that personal data is kept secure and not processed without proper authority, as summarised in Annex 1. The College observes legislative requirements and current best practice to ensure personal data is kept for no longer than necessary.

6.3 The College will not transfer personal data outside of the EEA unless it is satisfied that the data subject's rights under the DPA will be adequately protected.

6.4 The College would seek permission from an individual and, in the case of a pupil, his parents before allowing that person to feature particularly prominently in any media communications for which the College may give permission.

6.5 When processing personal data for the purposes set out above the College may communicate by post, email and SMS and may make use of third party software services.

7. THIRD PARTIES WITH WHOM THE COLLEGE MAY NEED TO SHARE PERSONAL DATA

From time to time the College may pass personal data (including sensitive personal data where appropriate) to third parties, including local authorities, other public bodies (eg the DBS, NCTL, UK Border Agency, HM Revenue and Customs, Department for Education and Department for Work and Pensions), independent school bodies such as the Independent Schools Inspectorate and the Independent Schools Council, school doctors and other health professionals, the College's professional advisers and its subsidiary Eton College Services Ltd (which is a data controller in

respect of the personal data it receives and processes and has notified its use of personal data with the ICO under registration number Z5862088), who will process the data:

- to enable the relevant regulatory authorities to monitor the College's performance;
- to compile statistical information (normally used on an anonymous basis);
- to secure funding for the College or on behalf of individual pupils;
- to safeguard pupils' welfare and provide appropriate pastoral (and, where relevant, medical) care;
- where specifically requested by pupils and/or their parents or guardians;
- where necessary in connection with learning and co-curricular activities undertaken by pupils;
- to enable pupils to take part in public examinations and other assessments and to monitor their progress and educational needs;
- to obtain appropriate professional advice and insurance for the School;
- where a reference or other information about a pupil or Old Etonian is requested by another educational establishment or employer to whom they have applied;
- where otherwise required by law; and
- otherwise where reasonably necessary for the operation of the School and employment of its staff.

The College will also share personal data about Old Etonians with the Old Etonian Association ("the OEA"); which may contact Old Etonians from time to time by post, email and SMS about the College and its activities. The OEA is a data controller in respect of the personal data it receives and processes and its ICO registration number is Z6801017.

8. RIGHTS OF ACCESS TO PERSONAL DATA

8.1 As data subjects, individuals have certain rights under the Data Protection Act, including a general right to be given access to personal data held about them by any data controller. The ICO's guidance is that, in the majority of cases, by the age of 12 an individual has sufficient maturity to understand his rights and to make an access request himself if he wishes.

8.2 If individuals wish to access their personal data held by the College or, in the case of parents, if they wish to access personal data held about their son or a pupil for whom they have parental responsibility, then a request should be submitted to the Data Protection Officer in writing. The College may charge an administration fee of £10 for providing this information.

8.3 The College aims to respond to such subject access requests as quickly as possible and will ensure that a response is provided within 40 days of receiving a valid request.

9. ACCURACY

The College will endeavour to ensure that all personal data held in relation to individuals is accurate and up to date. Individuals must notify the College of any changes to information held about them. An individual has the right to request that inaccurate information about them is corrected.

10. SECURITY

The College will take reasonable steps to ensure that personal data is kept secure and is only accessed by authorised members of its staff for the purposes for which it is held. All staff will be made aware of this Data Protection Policy and their duties under the DPA.

11. ENFORCEMENT

11.1 If an individual believes that the College has not complied with this Policy or has acted otherwise than in accordance with the DPA, the individual should notify the Data Protection Officer who shall, where appropriate, refer the matter for resolution in accordance with the College's grievance/ disciplinary procedure (for staff) or complaints procedure (for parents/ pupils).

11.2 This Policy forms part of the terms and conditions of all employees' contracts of employment. A breach of the policy may be regarded as misconduct, leading to disciplinary action up to and including summary dismissal. It also applies to all Fellows and other officers of the College and breach of this Policy may result in appropriate action being taken by the College.

12. GUIDANCE

Any queries about this Policy or how personal data is processed by the College should be referred to the Data Protection Officer for further guidance.

ANNEX 1

DATA SECURITY PRINCIPLES

- Access to personal data is provided to members of staff who require access to that personal data to perform their duties and responsibilities. As a result, different members of staff will have access to different categories of personal data depending upon their role.

- The security measures in place to protect data held electronically are set out in the College's Acceptable Use Policy, which is reviewed annually. All data on the Eton networks is protected by Sophos anti-virus software that runs on servers and workstations and is updated automatically. Data on the Eton networks is backed-up daily.

- Personal data held in manual files is only accessible by authorised individuals and, where of a confidential nature, is kept in locked filing cabinets when not in use.

- Paper-based copies of personal data (or other sensitive or confidential data) are disposed of in a secure manner, by shredding. Decommissioned IT equipment has data destruction procedures applied prior to its disposal.

- The physical security of the College premises is checked by the Security Department daily.

- The College ensures that prior to the transfer of any personal data to a third party for processing, the third party has appropriate technical and organisational security measures governing the processing to be carried out.

- New staff are required to read and understand the Acceptable Use Policy as part of their induction.

- Any lapses in data security must be reported to the IT Director at the earliest opportunity.