DATA PROTECTION AND PRIVACY POLICY

Introduction and duties

This policy applies to each of Queen's Kindergarten, Chapter House Preparatory School, King's Magna Middle School, Queen Ethelburga's College and The Faculty of Queen Ethelburga's, collectively referred to as the **Collegiate.**

The Collegiate or relevant part thereof is required, as part of its day to day operations, to process personal data about its current, prospective and former students and their parents, its current prospective and former staff, its suppliers/contractors, its current and prospective stakeholders and supporters, and other third party individuals connected to the Collegiate.

In doing so, the Collegiate is legally obliged to comply with the Data Protection Act 1998 (the **DPA**) when processing such personal data and will comply with the General Data Protection Regulation 2016 (**GDPR**), which will replace the DPA with effect from 25th May 2018 . This policy is intended to cover both the transitional period and the ensuing period, during which the GDPR comes in to force. Accordingly, the Collegiate will operate in accordance with the DPA until 25th May 2018 and thereafter in accordance with the GDPR, and the relevant provisions in the policy will apply as appropriate.

Personal data is any information which relates to an identified or identifiable living individual.
This policy sets out the basis on which any personal data the Collegiate collects, or that is provided to the Collegiate, will be processed by the Collegiate. The following should be carefully read to ensure the understanding of the views and practices of the Collegiate regarding personal data and how the Collegiate will process it.

An organisation that handles personal data and makes decisions about its use is known as a **Data Controller**. For the purposes of the DPA and the GDPR, the **Data Controller** is The Collegiate, Thorpe Underwood Hall, Ouseburn, York, YO26 9SS. For the purposes of the GDPR the Data Protection Officer is Mr C. Hall.

Information / personal data the Collegiate may process

Personal data processed by the Collegiate can take many different forms. It may be factual information, opinions, images or other types of information about a living individual. The Collegiate may collect and process, for example, the following information/data:

- For all, general personal data such as name, address, contact details (including, without limitation, telephone number, mobile telephone number, e-mail address).
- For staff and contractors or other suppliers, additional information required for their employment/appointment including images, audio and video recordings and biometric data, Disclosure and Barring Service record checks (as legally required for the purposes of working with children) and/or basic checks for confirming suitability for the post.
- For students, admissions, academic, pastoral, 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, and agents, employment details and financial information.
- Sensitive personal data processed by the Collegiate about an individual includes data concerning their physical or mental health or condition, ethnic group, religious beliefs, political beliefs, criminal records and proceedings, trade union membership and relevant medical information.
- CCTV images for security purposes, health and safety obligations and insurance requirements.

Generally, the Collegiate collects personal data it processes directly from the subject of that data (or, in the case of a student, his/her parents, guardians or agents) (**Data Subject**). However, the Collegiate may receive information about a Data Subject from third parties (including, for example, the Disclosure and Barring Service, referees, business partners, sub-contractors, search information providers, credit reference agencies). Personal data held will be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (**Data Minimisation**).

Purposes for which information/personal data collected may be used

Personal data (including sensitive personal data, where appropriate) is processed by the Collegiate in accordance with the relevant legislation for the following purposes:

- **The provision of education** including the registration of prospective students and administration of the admissions process; administration of the school curriculum and timetable; administration of student entries to public examinations, reporting upon and publishing the results; providing references for students and preparation of information for inspections.
- **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 school trips; boarding house administration; monitoring of student's e-mail communications, internet use and telephone calls. This may include online identifiers.
- **Information required by the UK Visas and Immigration, where applicable.**
- **The general administration of the Collegiate** including the compilation of student records; the administration of invoices, fees, bursaries, awards and accounts; the management of the Collegiate's property; the management of security and safety arrangements (including use of CCTV); the administration and implementation of the policies of the Collegiate and other reasonable purposes related to the operations of the Collegiate.
- **The protection and promotion of the legitimate interests and objectives of the Collegiate** including the publication of its website, the prospectus, publications, fundraising for charitable

and other purposes, the maintenance of historic archives and communicating with former students.

- **The administration of the staff, agents and suppliers of the Collegiate** including recruitment of staff / engagement of contractors. This will include compliance with Disclosure and Barring Service checks, or such similar checks or services, payroll administration, pension administration, health administration, health insurance/benefits, training and appraisal including performance and disciplinary records and equal opportunities monitoring, and the maintenance of appropriate human resources records for current and former staff, and providing references.
- **Compliance with the Collegiate's contractual and other legal obligations.**

Testing and Examinations

In order to administer national tests, the Collegiate are required to pass on some personal data to the bodies responsible for the National Curriculum and associated assessment arrangements.
Parents are informed that, if the Collegiate is not granted permission to pass on such personal data (whether via the Parent Portal or otherwise), it is unable to enter the student for public examinations.

The results of national tests are passed on to the Department of Education in order to compile statistics on trends and patterns in levels of achievement, to evaluate the effectiveness of the National Curriculum and the associated assessment arrangements, and to ensure that these are continually improved. The Collegiate will provide only information required by law to any Government Agency or the like.

Processing of Personal Data

The purpose for collecting data will be clearly identified. The Collegiate 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 (and as outlined in this policy) and will not process it for any other purpose without permission, unless permitted to do so under the relevant legislation or required to do so by law. The Collegiate may communicate with Data Subjects by post, email, telephone, SMS (or other electronic messaging service).

The Collegiate will obtain personal data only by lawful and fair means, and, where appropriate, with the knowledge and consent of the individual concerned. Some data may already have been made public by the Data Subject, but where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their personal data, the Collegiate will seek such freely-given consent. Such consent can be withdrawn at any time.

Personal data shall only be disclosed to those staff members, contractors, subcontractors, suppliers, or agents who need to access the personal data to carry out the purposes for which it was acquired. The Collegiate adopts appropriate reasonable physical, technical and organisational security measures to ensure that personal data is kept secure and not processed without proper authority. Where appropriate, the Collegiate will use encryption of information.

The Collegiate will not transfer personal data outside of the European Economic Area unless it is satisfied that the Data Subject's rights under the relevant legislation will be adequately protected. The Collegiate would seek permission from an individual and, in the case of a student under 16, his/her parents/guardian before allowing that person to feature particularly prominently in documentary films or articles for which the Collegiate may give permission. When processing personal data for the purposes set out above, the Collegiate may communicate by post, email and SMS (or other electronic messaging service) and may make use of cloud computing services.

Staff Training

Staff handling personal data will have their responsibilities under this policy outlined to them as part of their induction and as part of procedural update training. Training will include the following elements, as appropriate to the role of the staff:

- Employees' duty to use and permit the use of personal data only by authorised persons and for authorised purposes;
- the need for, and proper use of, the forms and procedures needed to implement this policy;
- the correct use of passwords, logging out, and other access mechanisms;
- secure storage of manual files, print-outs and electronic storage media;
- the need for appropriate safeguards for all transfers of personal data outside the internal network and physical Collegiate premises;
- proper disposal e.g. by shredding.

The Collegiate may share personal data with certain third parties

From time to time, the Collegiate may pass personal data (including sensitive personal data where appropriate) to third parties, including local authorities; other public bodies (e.g. the DBS, UK Visas and Immigration, 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; health professionals; insurers; debt collection agencies; former and prospective schools and employers; other associated businesses; and the Collegiate's professional advisers who will process the data:

- to enable the relevant authorities to monitor the Collegiate's performance;
- to compile statistical information (normally used on an anonymous basis);
- to secure funding for the Collegiate or student, on behalf of individual students;
- to safeguard students' welfare and provide appropriate pastoral (and, where relevant, medical) care;
- where specifically requested by students and/or their parents or guardians;
- where necessary in connection with learning and co-curricular activities undertaken by students;
- to enable students 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 Collegiate;

- to collect outstanding debts;
- where a reference or other information about a student or former student is requested by another educational establishment or employer to whom they have applied;
- to process payroll and charitable awards;
- where otherwise required by law, regulation, or court order; and
- otherwise where reasonably necessary for the operation of the Collegiate and employment of its staff.

If appropriate, safeguards such as anonymisation or pseudonymisation will be employed to remove the possibility of identification.

Staff Information

Data concerning staff will be confidentially and securely stored, in personal files, which are subject to access only by those needing to work with them. In order to comply with regulations governing staffing of schools, a Central Register of key professional information is kept, with restricted access. Staff may ask to see their personal files, with the exception of any data which might compromise another individual's right to privacy or make it difficult to detect a crime. Applicants for jobs will be made aware of what information is being collected, and why, and respect for personal privacy will be observed. Legal obligations for disclosure of information will supersede the protection of privacy, unless they are subject to an exemption. Data collected for monitoring purposes will be retained only for the designated purpose, will be kept securely, and will be destroyed securely, once no longer needed.

Parent Portal

The School operates an online Parent Portal, which provides a secure environment for communicating with parents and guardians, including in relation to authorisations for extra lessons, activities, and personal weekend visits, along with providing school reports, examination results, and allowing other correspondence between the Collegiate and parents/guardians.

Due to the nature of this system, certain personal data may be accessible by those persons granted access to the system.

The School will therefore only grant access to, and add personal data to, the Parent Portal with consent. Consent will be expressly given in writing by the joint signatories on the registration form enrolling a student with the Collegiate, and the School may enter any personal data provided on such form and subsequently provided by a joint signatory thereto onto the Parent Portal unless notified otherwise or if consent is at any time withdrawn.

The School will not grant access to the Parent Portal to any person who is not a joint signatory to the registration form enrolling a student with the Collegiate without the prior consent of the persons with existing access to the Parent Portal.

In the event that access to the Parent Portal or personal data or information contained therein is to be restricted (such as, for example, following family breakdown) the Data Subject and/or parent/guardian should immediately contact the Principal/Data Protection Officer (DPO).

Rights of access to personal data

Data Subjects have certain rights under the relevant legislation, including a general right to be given access to personal data held about them by any Data Controller. Certain conditions apply under the DPA in relation to the making of a subject access request and further information can be obtained from the Principal. These provisions will continue to apply for any requests received by the Collegiate before 25th May 2018.

If individuals wish to access their personal data held by the Collegiate or, in the case of parents/guardians, if they wish to access personal data held about their child or a student for whom they have parental responsibility, then a request should be submitted to the Principal or DPO in writing, and the Collegiate is entitled to ask for any further information, reasonably required, to locate the information and satisfy itself about the identity of the person making the request.

There is no charge for access to information under the GDPR, unless the request is deemed excessive, in which case the Collegiate may charge an administration fee for providing this information. The Collegiate aims to respond to such subject access requests as quickly as possible, and within one month of any requested further information regarding the identity or location of the information being received (unless an exemption from the right of access under the GDPR applies). If it is not possible to respond fully to the request within **one month**, the Collegiate will acknowledge receipt of the request, giving reasons for the refusal and any procedures available for appealing the decision, an estimate of costs to be paid where the request is excessive in nature, and an estimated date by which any remaining responses will be provided.

Children

As a general guide, by the age of 13 an individual is deemed by the Collegiate to have sufficient maturity to understand his/her rights and to make an access request although the Collegiate will consider such requests on a case-by-case basis. If the individual cannot understand the nature of the request, someone with parental responsibility can ask for the information on the child's behalf and receive the response. When a request is received from a child, for access to their own information, those responsible for responding should take into account whether:

- the child wants their parent (or someone with parental responsibility for them) to be involved in the request; and
- the child properly understands what is involved in making the request and the type of information they will receive.

Where the response includes information about another individual, the request will be considered carefully. There is a duty to consider the rights of the individual making the request and the privacy of any other individuals who may be identified.

Under the subject access right, parents will only be able to see all the information about their child when the child is unable to act on their own behalf or gives their consent. They should be aware that they may not be consulted.

Rights of access to educational record

The Collegiate recognises that a parent has the right to access their child's educational record. The educational record is confined to information that comes from a teacher or other employee of a

school, the student or their parents. Communications about a particular child from head teachers and teachers at a school and other employees at an education authority will therefore form part of that child's official educational record, as will correspondence from an educational psychologist engaged by the Principal under a contract of services. It may also include information from the child and their parents, such as information about the health of the child.

Information kept by a teacher solely for their own personal use does not form part of the official educational record.

The Collegiate will respond to requests for information from students, or parents, for information that contains, wholly or partly, an educational record **within 15 working days.**

Requests from parents to view their child's educational record, or from students, or someone acting on their behalf, requesting personal information, should be dealt with by the Principal.

Withholding of Information
The Collegiate may withhold certain information if:

- the information relates to:
    - information which might cause serious harm to the physical or mental health of the student or another individual;
    - cases where the disclosure would reveal a child is at risk of abuse;
    - information contained in adoption and parental order records;
    - information given to a court in proceedings under the Magistrates' Courts (Children and Young persons) Rules 1992;
    - copies of examination scripts; and
    - providing examination marks before they are officially announced.
- the request is for unstructured personal information. Where the request is for unstructured personal information, the Collegiate is entitled to ask for a description of the information to help them find it. They do not have to supply the information, or confirm whether or not it exists, if it would cost more than £450 to do either of these things. This cost structure is in The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004.

Rights to withdraw consent, prevent direct marketing, correct inaccuracies, request erasure and the right to data portability under GDPR
Under GDPR, permission to process personal data for purposes of fundraising or direct marketing can be withdrawn by the Data Subject. (Where marketing is carried out in a business-to-business context, there is no legal requirement to obtain an indication of consent to carry out marketing to individuals, provided that they are given the opportunity to opt out.)

The Collegiate will adopt all necessary measures to ensure that the personal data it collects and processes is complete and accurate in the first instance and is updated. Individuals have the right to

request that personal data that is inaccurate or incomplete be amended or removed. This should be done within one month of the request, unless it is complex.

Under certain conditions, a request can also be made to erase personal data (including by any third party who processes or uses that data on behalf of the Collegiate), if there is no longer any legitimate reason for it to be retained or a further exemption applies.

Data Subjects have the right to obtain, reuse and transmit their data to another data controller free of charge. Data subjects can therefore receive personal data which they have provided to the Collegiate in a structured and commonly used and machine readable format, if the data is in automated form and can request the Collegiate to transmit it to another data controller. The Collegiate will respond to requests for portability without undue delay and within one month. This can be extended to two months where the request is complex or a number of requests are received. Any refusals will be explained and the data subject will be advised of their right to complain to the Information Commissioners Office (ICO).

Data Retention

Data will be retained only for as long as is necessary, either for the purpose for which it was intended or to meet statutory obligations (See examples in Appendix). It will be disposed of securely, when no longer needed.

Data Breach

The GDPR places an obligation on organisations to report data breaches that reach certain thresholds and subject to certain exceptions (for example where the compromised data was rendered intelligible due to encryption) . A data breach that is likely to result in a risk to the rights and freedoms of individuals must be notified to the appropriate authority (ICO) normally within 72 hours of the Collegiate becoming aware of the breach. Where that is a high risk, individuals will be notified directly and without undue delay. Any individual who suspects that a personal data breach has occurred, e.g. due to theft or accidental loss should notify the Principal/DPO immediately, providing a description of what has occurred. All reported incidents will be investigated, to confirm whether or not a personal data breach has occurred, and appropriate action will be taken.

Queries and Complaints

Any queries on this policy should be directed to the Principal/DPO. If an individual believes that the Collegiate has not complied with this policy or has acted otherwise than in accordance with the relevant legislation, they should utilise the Collegiate complaints procedure, available on the Parent Portal or on request. Data Subjects also have the right to complain to the ICO.

Related Policies

This policy should be read in conjunction with other policies which can relate to the confidentiality of information:

- Medical Policy
- Safeguarding Policy
- Safe Recruitment Policy
- Pastoral Care Policy

- Equal Opportunities Policy
- Anti-Bullying Policy
- CCTV Policy
- Acceptable Use Policy
- E-safety Policy

Reviewed August 2017
To be reviewed 25 May 2018

Appendix – Examples of retention periods for data (Provided by the ISBA)

Type of Record/Document	**Suggested 1 Retention Period**
SCHOOL-SPECIFIC RECORDS Registration documents of School	Permanent (or until closure of the school)
Attendance Register	6 years from last date of entry, then archive.
Annual curriculum	From end of year: 3 years (or 1 year for other class records: e.g. marks / timetables / assignments)
INDIVIDUAL PUPIL RECORDS	***NB - this will generally be personal data***
Admissions: application forms, assessments, records of decisions	25 years from date of birth (or, if pupil not admitted, up to 7 years from that decision).
Examination results (external or internal)	7 years from pupil leaving school
Pupil file including: o Pupil reports o Pupil performance records o Pupil medical records	ALL: 25 years from date of birth* * *unless there is good reason to consider this may be applicable evidence in a medical negligence or abuse claim*.
Special educational needs records (*to be risk assessed individually*)	Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period)
SAFEGUARDING	
Policies and procedures	Keep a permanent record of historic policies
DBS disclosure certificates (potentially sensitive personal data & must be secure)	No longer than 6 months from decision on recruitment, unless specific DBS reason for retention.
EMPLOYEE / PERSONNEL RECORDS Contracts of employment	***NB this will almost certainly be personal data*** Minimum - 7 years from effective date of end of contract
Employee appraisals or reviews and staff personnel file	Duration of employment plus minimum of 7 years