G2 Data Protection Policy

What is this policy for?

This policy is intended to provide information about how the Purcell school will use (or "process") personal data about individuals including: its staff; its current, past and prospective students; their parents, carers or guardians (referred to in this policy as "parents"); supporters of the School (including Friends of the Purcell School, donors and Trust Funds)

This information is provided in accordance with the rights of individuals under Data Protection Law to understand how their data is used. Staff, parents and students are all encouraged to read this policy and understand the school's obligations to its entire community.

This policy applies alongside any other information the school may provide about a particular use of personal data, for example when collecting data via an online or paper form.

This Policy also applies in addition to the School's other relevant terms and conditions and policies, including:

- the School's terms and conditions
- the school's policy on taking, storing and using images of children;
- the school's CCTV policy;
- the school's safeguarding and pastoral policies, including as to how concerns or incidents are recorded;
- the school's health and safety policies,
- the school's IT policies, including its Acceptable Use policy and E-Safety policy
- the School's Fundraising Policy.
- Privacy notices which outline how data is used in specific areas of the School.

Responsibility for Data Protection

The School has appointed the Bursar as the Chief Privacy Officer. The CPO:

- Will oversee the implementation of this policy and the monitoring of its effectiveness.
- Will co-ordinate requests and enquiries concerning the school's uses of personal data (see section on Your Rights below)
- Will endeavour to ensure that all personal data is processed in compliance with this policy and Data Protection Law.
- Will ensure each key area of the School (HR, Fundraising, Academic, Pastoral, ICT, Governance, Admissions and Student Data) appoints a Data Handler who will, in conjunction with their Line Manager and seeking advice from the Bursar, implement this policy in their area.
- Will ensure colleagues in their area are aware of this policy and are following the procedures outlined.
- Will act as the first point of contact for dealing with issues.
- Will ensure GDPR is an agenda item at the SLT meeting once per term.
- All staff are responsible for reporting any data breaches to the Bursar.
- Governors will consider GDPR issues annually through the annual risk management review process at the Finance and General Purposes Committee meeting and any concerns will be referred to the Governing body.

Why the School Needs to Process Personal Data

In order to carry out its ordinary duties to staff, students, parents and Supporters the school may process a wide range of personal data about individuals (including current, past and prospective staff, students or parents) as part of its daily operation.

Some of this activity the school will need to carry out in order to fulfil its legal rights, duties or obligations – including those under a contract with its staff, or parents of its students.

Other uses of personal data will be made in accordance with the school's legitimate interests, or the legitimate interests of another, provided that these are not outweighed by the impact on individuals, and provided it does not involve special or sensitive types of data.

The school expects that the following uses may fall within that category of its (or its community's) "**legitimate interests**":

- For the purposes of student selection (and to confirm the identity of prospective students and their parents);
- To provide education services, including musical education, physical training or spiritual development, career services, and extra-curricular activities to students, and monitoring students' progress and educational needs;
- Maintaining relationships with alumni, the school community and supporters including direct marketing or fundraising activity;
- For the purposes of management planning and forecasting, research and statistical analysis, including that imposed or provided for by law (such as diversity or gender pay gap analysis and taxation records);
- To enable relevant authorities to monitor the school's performance and to intervene or assist with incidents as appropriate;
- To give and receive information and references about past, current and prospective students, including relating to outstanding fees or payment history, to/from any educational institution that the student attended or where it is proposed they attend; and to provide references to potential employers of past students;
- To enable students to take part in national or other assessments, and to publish the results of public examinations or other achievements of students of the school;
- To safeguard students' welfare and provide appropriate pastoral care;
- To monitor (as appropriate) 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 students 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, including CCTV in accordance with the school's CCTV policy; and
- Where otherwise reasonably necessary for the school's purposes, including to obtain appropriate professional advice and insurance for the school.

In addition, the school may need to process special category personal data (concerning health, ethnicity, religion, biometrics or sexual life) or criminal records information (such as when carrying out DBS checks) in accordance with rights or duties imposed on it by law, including as regards safeguarding and employment, or from time to time by explicit consent where required. These reasons may include:

- To safeguard students' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency, incident 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, social services, insurance purposes or to organisers of school trips;
- To provide educational services in the context of any special educational needs of a student;
- In connection with employment of its staff, for example DBS checks, welfare or pension plans;
- For legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with its legal obligations and duties of care.

Types of Personal Data Process by the School

This will include 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 students' 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 students, and information provided by previous educational establishments and/or other professionals or organisations working with students; and
- images of students (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)

Who has Access to Personal Data and Who the School Shares it With

Occasionally, the school will need to share personal information relating to its community with third parties, such as professional advisers (lawyers and accountants) or relevant authorities (HMRC, police or the local authority).

For the most part, personal data collected by the school will remain within the school, and will be processed by appropriate individuals only in accordance with access protocols (i.e. on a 'need to know' basis). Particularly strict rules of access apply in the context of:

- medical records held and accessed only by the school nurse and appropriate medical staff under his/her supervision, or otherwise in accordance with express consent];
- pastoral or safeguarding files.

However, a certain amount of any SEN student's relevant information will need to be provided to staff more widely in the context of providing the necessary care and education that the student requires.

Staff, students and parents are reminded that the school is under duties imposed by law and statutory guidance (including Keeping Children Safe in Education) to record or report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, if they meet a certain threshold of seriousness in their nature or regularity. This may include file notes on personnel or safeguarding files, and in some cases referrals to relevant authorities such as the LADO or police. For further information about this, please view the school's Safeguarding Policy.

Finally, in accordance with Data Protection Law, some of the school's processing activity is carried out on its behalf by third parties, such as IT systems, web developers or cloud storage providers. This is always subject to contractual assurances that personal data will be kept securely and only in accordance with the school's specific directions.

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, or alumni and parent events of interest, including by sending updates and newsletters, by email and by post. Unless the relevant individual objects, the school may also:

- Contact parents and/or alumni by post and email in order to promote and raise funds for the school and, where appropriate, other worthy causes;
- Should you wish to limit or object to any such use, or would like further information about them, please contact the Bursar in writing. You always have the right to withdraw consent, where given, or otherwise object to direct marketing or fundraising. However, the school may need nonetheless to retain some of your details (not least to ensure that no more communications are sent to that particular address, email or telephone number).

Your Rights

Individuals have various rights under Data Protection Law to access and understand personal data about them held by the school, and in some cases ask for it to be erased or amended or for the school to stop processing it, but subject to certain exemptions and limitations.

Any individual wishing to access or amend their personal data, or wishing it to be transferred to another person or organisation, or who has some other objection to how their personal data is used, should put their request in writing to the Bursar.

The school will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event within statutory time-limits, which is one month in the case of requests for access to information. The school will be better able to respond quickly to smaller, targeted requests for information. If the request is manifestly excessive or similar to previous requests, the school may ask you to reconsider or charge a proportionate fee, but only where Data Protection Law allows it.

You should be aware that certain data is exempt from the right of access. 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 student examination scripts (though examiners' comments may be disclosed), nor any confidential reference given by the school for the purposes of the education, training or employment of any individual.

Student Requests

Students 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 (see section Whose Rights below). Indeed, while a person with parental responsibility will generally be entitled to make a subject access request on behalf of younger students, the information in question is always considered to be the child's at law.

A student of any age may ask a parent or other representative to make a subject access request on his/her behalf. Moreover (if of sufficient age) their consent or authority may need to be sought by the parent making such a request. Students aged 13 and above are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested, including any relevant circumstances at home. Slightly younger children may however be sufficiently mature to have a say in this decision.

All information requests from, or on behalf of, students – whether made under subject access or simply as an incidental request – will therefore be considered on a case by case basis.

Consent

Where the school is relying on consent as a means to process personal data, any person may withdraw this consent at any time (subject to similar age considerations as above). Please be aware however that the school may have another lawful reason to process the personal data in question even without your consent.

That reason will usually have been asserted under this policy, or may otherwise exist under some form of contract or agreement with the individual (e.g. an employment or parent contract, or because a purchase of goods, services or membership of an organisation such as an alumni or parents' association has been requested).

Whose Rights

The rights under Data Protection Law belong to the individual to whom the data relates. However, the school will often rely on parental consent to process personal data relating to students (if consent is required) unless, given the nature of the processing in question, and the student's age and understanding, it is more appropriate to rely on the student's consent.

Parents should be aware that in such situations they may not be consulted, depending on the interests of the child, the parents' rights at law or under their contract, and all the circumstances. In general, the school will assume that students' consent is not required for ordinary disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the student's activities, progress and behaviour, and in the interests of the student's welfare, unless, in the school's opinion, there is a good reason to do otherwise.

However, where a student 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 may be under an obligation to 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 student or other students, or if required by law.

Students are required to respect the personal data and privacy of others, and to comply with the school's IT: acceptable use policy and the school rules. Staff are under professional duties to do the same covered in the Staff Handbook.

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 please notify the relevant person outlined in the relevant of any significant changes to important information, such as contact details, held about them.

An individual has the right to request that any out-of-date, irrelevant or inaccurate or information about them is erased or corrected (subject to certain exemptions and limitations under Data Protection Law): please see above for details of why the school may need to process your data, of who you may contact if you disagree.

The school will take appropriate technical and organisational steps to ensure the security of personal data about individuals, including policies around use of technology and devices, and access to school systems. All staff and governors will be made aware of this policy and their duties under Data Protection Law and receive relevant training.

Relevant Legislation

The School will endeavour to ensure that all data is processed in compliance with the following legislation:

- The General Data Protection Regulation (from 25 May 2018)
- The Data Protection Act 2018 and related legislation (from 25 May 2018, form TBC)
- The Privacy and Electronic Communications Regulations 2011 (PECR) (to continue after 25 May 2018 until replaced by the ePrivacy Regulation – form and date TBC)
- The Protection of Freedoms Act 2012 (biometrics and CCTV)

In addition the School will take note of the guidance and practice notes provided by the Information Commissioner's Office [A1] ("ICO") (*final guidance on consent and legitimate interests expected to follow from December 2017*):

- Privacy Notices, Transparency and Control (ICO Guidance, drafted in anticipation of GDPR but not a full GDPR Privacy Notices Code of Practice)
- Privacy Notices under the GDPR (short-form guidance with checklist)
- The ICO sector-specific guidance for schools, universities and colleges
- Direct Marketing Guidance (PECR) (last updated April 2016 but still applicable after GDPR)
- The Subject Access Code of Practice (last updated June 2017)
- The ICO Code of Practice on CCTV (last updated June 2017)
- The ICO's Guide to Data Protection
- Overview of the General Data Protection Regulation (short-form overview)
- DRAFT Consent Guidance for GDPR (final text expected by end of 2017)

This Policy

The school will update this Data Protection and Privacy Policy from time to time. Any substantial changes that affect your rights will be provided to you directly as far as is reasonably practicable.

Queries and Complaints

Any comments or queries on this policy should be directed to the Bursar.
If an individual believes that the school has not complied with this policy or acted otherwise than in accordance with Data Protection Law, they should utilise the school complaints / grievance procedures and should also notify the Bursar. The school can also make a referral to or lodge a complaint with the Information Commissioner's Office (ICO), although the ICO recommends that steps are taken to resolve the matter with the school before involving the regulator.

Policy author / reviewer:	***Policy date / review date:***	***Next review due:***
Aideen McNamara	May 2018	
Paul Bambrough	January 2020	January 2021

G2 Appendix – GDPR Retention and Disposal Schedule

Information Type	Retention Trigger	Retain For	Action	Information Asset Owner
Information created in relation to new policies, guidelines and research. This information has been created internally to guide decision making. This relates to any final drafts and significant supporting information	Last Action	6 Years	Destroy	Data Manager / IT Manager
Engagement with significant stakeholders: This will include government departments, large companies and charities as well as international work	Last Action	6 Years	Review	Bursar
Internal Committees and Groups minutes	Last Action	6 Years	Destroy	Principal's PA
Health and Safety Inspections, Property Management and Asset Records	Last Action	6 Years	Review	Estates Manager
Documents relating to IT system	End of System Life	12 Months	Review	IT Manager
Building Reports, Risk Assets, Helpdesk and Security Reports	Last Action	3 Years	Review	Estates Manager
IT Back ups	Last Action	6 Month	Destroy	IT Manager
CCTV	Last Action	1 Month	Destroy	IT Manager
Reception Sign in Book / "Inventry System"	End of Year	2 Years	Destroy	Data Manager / IT Manager
Financial Information	End of Financial Year	6 Years	Destroy	Finance Manager
Payroll Iris System Data	End of Financial Year	6 Years	Destroy	Deputy Bursar
Employee Files and Personal Development Records	End of Employment	6 Years	Destroy	HR Manager
Disciplinary and Grievance, Examination and Testing, Accident and Ill Health	Last Action	6 Years	Destroy	HR Manager
Job Descriptions and Terms & Conditions	Last Action	6 Years	Destroy	HR Manager
Training Material	Last Action	6 Years	Destroy	HR Manager
General Annual Leave Information	End of Financial Year	3 Years	Destroy	HR Manager
Maternity, Paternity, Adoption and Sick Leave	End of Financial Year after return	3 Years	Destroy	HR Manager
Successful Recruitment Candidate Information (including third party referee details provided by the applicant)	End of Employment	6 Months	Destroy	HR Manager
Unsuccessful Recruitment Candidate Information (including third party referee details provided by the applicant)	Last Action	6 Months	Destroy	HR Manager
Staff Pension, Pay History, and Termination Reasons	From DOB	100 Years	Destroy	HR Manager
Medical/Self Certificates	End of absence	4 Years	Destroy	HR Manager
Market Research Reports, Press Releases, Campaigns and Projects,	Last Action	6 Years	Review	Marketing Manager

Information Type	Retention Trigger	Retain For	Action	Information Asset Owner
Legal Advice	Last Action	6 Years	Review	Bursar
Contracts	End of Contract	6 Years	Review	Finance Manager
Non–disclosure agreements	Last Action	2 Years	Review	Bursar
Staff Mailboxes and Outlook	End of Employment	12 Months	Destroy	IT Manager
Physical Correspondence	Once Scanned	6 Months	Destroy	Document owner
Internal Email Mailboxes	End of Employment	12 Months	Destroy	IT Manager
Student Email Boxes	Creation	12 Months	Destroy	IT Manager
Management Information	End of Financial Year	6 Years	Review	Principal's PA
Data Protection and FOI Complaints	Case Closed	2 Years	Destroy	Bursar
DBS	Last Action	6 Months	Destroy	HR Manager
Serious safeguarding incidents (IICSA)	Last Action	Indefinitely unless advised otherwise	Review	DSL
Safeguarding	Last Action	At least until the accused has reached normal pension age or for 10 years from the date of allegation if this is longer (DfE, 2020)	Review/ Destroy	DSL