Data Protection Policy

Date first Published:	New policy
Version:	1
Ownership:	Head of Finance
Author:	Danni Laing
Signed by Governors:	June 2016

History of Policy Changes

Date	Version	Change	Origin of Change e.g. TU request, change in legislation	Changed by
June 2016	1	New policy		DL

Contents

Clause

1. Policy statement

1.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our students, staff (which will include permanent, temporary employees and volunteer staff, consultants and contractors), parents/carers and clients, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2 Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

2. About this policy

2.1 The types of personal data that Priory Community School (We) may be required to handle include information about current, past and prospective staff (as defined above), students, parents/carers and others that we communicate with. The personal data, which may be held on paper or on computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations.

2.2 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy has been approved by the Governing Body. It sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.5 The Data Protection Compliance Manager is responsible for ensuring compliance with the Act and with this policy. That post is held by the Head of Finance, Martin Kerslake. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Compliance Manager.

3. Definition of data protection terms

3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data subjects** include all living individuals about whom we hold personal data.

3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.4 **Data controllers** are the people who or the organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

3.5 **Data users** are those of our staff (which means our employees, governors, contractors and consultants) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

3.6 **Data processors** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. This includes our payroll service agents, pension providers and legal and professional advisors.

3.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

4. Data protection principles

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

(a) Processed fairly and lawfully.

(b) Processed for limited purposes and in an appropriate way.

(c) Adequate, relevant and not excessive for the purpose.

(d) Accurate.

(e) Not kept longer than necessary for the purpose.

(f) Processed in line with data subjects' rights.

(g) Secure.

(h) Not transferred to people or organisations situated in countries without adequate protection.

5. Fair and lawful processing

5.1 The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

5.2 For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Act. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed.

5.3 When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

6. Processing for limited purposes

6.1 In the course of our business, we will collect and process personal data. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, parents/carers/family members, health professionals, business partners, regulatory authorities (eg. Disclosure & Barring Service, Police, social services, local authority), previous employers, credit reference agencies and others).

6.2 We will only process personal/sensitive personal data for purposes specifically permitted by the Act, including but not limited to:

- The provision of education
- Employment – effective human resource management – recruitment (vetting and verifying applications), equal opportunities monitoring, the management of grievance and disciplinary matters, employment reference provision, performance management
- Statutory obligations – reporting and monitoring obligations, recruitment (e.g. *Keeping Children Safe in Education 2015)*, performance management (teachers - *Education (School Teachers' Appraisal) (England) Regulations 2012*)
- Health management – sickness absence monitoring, occupational health referrals, early/ill health retirement applications, special educational needs management
- Financial – payroll, pensions, insurances, funding applications.

7. Adequate, relevant and non-excessive processing

We will only collect personal data to the extent that it is required for the specific purpose.

8. Accurate data

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

9. Timely processing

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

10. Processing in line with data subject's rights

We will process all personal data in line with data subjects' rights, in particular their right to:

(a) Request access to any data held about them by a data controller (see also clause 14).

(b) Prevent the processing of their data for direct-marketing purposes.

(c) Ask to have inaccurate data amended (see also clause 8).

(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

11. Data security

11.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

11.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

11.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the School's central computer system instead of individual PCs.

11.4 Security procedures include:

(a) **Entry controls.** Any stranger seen in entry-controlled areas should be reported.

(b) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(c) **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

(d) **Passwords.** All staff will have individual, confidential passwords for access to their IT and communication equipment, memory sticks, software, cloud based storage and electronic files containing personal data.

(e) **Encryption**. All staff will be encouraged to:

- encrypt files containing personal data before transmitting them electronically outside of the School network including cloud storage;
- encrypt and password protect the contents of any memory stick containing personal data.

(f) **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they lock/log off from their PC when it is left unattended.

(g) **Security.** All staff will be discouraged from leaving their laptop computers, school files/work unattended in their vehicles or on public transport, where there is an increased risk of theft.

(h) **Cloud service providers.** We conduct a privacy impact assessment to include ensuring that we obtain a contract and/or data processing agreement which confirms the cloud service provider complies with the requirements of the DPA.

(i) **Confidentiality agreements.** We will require all staff, consultants, contractors and volunteers who have access to personal data held by the School to enter into contractual agreements with the School to protect and preserve confidentiality and to comply with the terms of this Data Protection Policy.

12. Transferring personal data to a country outside the EEA

12.1 We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

(a) The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.

(b) The data subject has given his consent.

(c) The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.

(d) The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.

(e) The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

12.2 Subject to the requirements in clause 11.1 above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

13. Disclosure and sharing of personal information

13.1 We may share personal data we hold with our subsidiary (trading) company, Priory Community School Enterprises for the purposes of staff secondment and their provision of health and safety services to the School.

13.2 We may also disclose personal data we hold to third parties:

(a) such as another school, college or university which requires information about the data subject’s education, achievements or needs;

(b) in the event that we acquire any business or assets, in which case we may disclose personal data we hold to the owner of such business or assets;

(c) if we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets;

(d) such as the provider of hosted/online educational software or business services where the provision of personal data supports login/access arrangements (for example, Google, Microsoft, GCSEPod) (Appendix A);

(e) for the purposes of obtaining professional advice (for example, legal, educational, health and welfare advice) for ourselves and/or the data subject;

(f) if we are under a duty to disclose or share a data subject's personal data in order to comply with any legal or regulatory obligation; for example, to:

- OfSTED
- Police, Disclosure & Barring Service, National College for Teaching & Leadership
- Local Authority
- Children's and Social Services
- HMRC, Department of Work & Pensions, Avon Pension Fund/Local Government Pension Scheme.
- Occupational health service providers, employee assistance programme providers
- Education Funding Agency;
- Health Authority;

(g) in order to enforce or apply any contract with the data subject; and

(h) to protect our rights, property, or safety of our employees, students, parents/carers or others.

13.3 We will, wherever possible, prior to disclosing any personal data, obtain written confirmation from the third party that it will:

- not itself share such personal data with any third party;
- keep the personal data confidential;
- comply with the requirements of this policy and any additional relevant provisions of the Data Protection Act.

14. Dealing with subject access requests

14.1 Data subjects must make a formal request for information we hold about them. This must be made in writing and submitted to the School's Main Office, marked for the attention of the Data Protection Compliance Officer.

14.2 Provided that there is sufficient information to process the request, an entry will be made in the Subject Access log book, showing the date of receipt, the data subject's name, the name and address of the requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date).

14.3 Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be the date on which sufficient information has been provided.

14.4 The identity of the requestor must be established before the disclosure of any information, and checks should be carried out regarding proof of relationship to the student. Evidence of identity can be established by requesting production of (this list is not exhaustive): passport, driving licence, utility bills with current address, Birth / Marriage Certificate, P45/P60, Credit Card or Mortgage statement.

14.5 Where a request for subject access is received from a student, the School's policy is that:

- The requested information will be given directly to the student, unless it is clear that the student does not understand the nature of the request;
- Requests from students who do not appear to understand the nature of the request will be referred to their parents or carers; and
- Requests made from parents or carers in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent or carer.

14.6 In the case of any written request from a parent/carer regarding their own child's record, access to the record will be provided within 15 school days in accordance with the current Education (Pupil Information) Regulations 2005.

14.7 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

(a) We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

14.8 Our employees will refer a request to the Data Protection Compliance Manager for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

15. CCTV

We have Closed Circuit Television (CCTV) on the School site for the purposes of security and safety and, to monitor that student and staff behaviour and conduct complies with our policies and procedures.

The School has a CCTV Usage Policy, a copy of which is available from the School website (and staff intranet).

Images recorded by the CCTV system are stored, processed and destroyed in accordance with the "ICO Code of Practice 2015 for surveillance cameras and personal information".

16. Photographs/video images

16.1 The School uses photographs and video images of students (which may or may not be accompanied by their forename) for the purposes of:

- education, teaching and learning;
- communication and information sharing;
- student recognition and reward;
- marketing and publicity (including but not limited to, news and press reporting, school prospectuses, webcasts/podcasts and annual reports, banner displays and hoardings)
- security and staff and student safety.

16.2 Each academic year parents/carers are asked, whether they object to the School (and thereby its authorised staff) taking and using photographs and video images of their child for school related purposes. The School assumes that consent is granted in the absence of an objection.

16.3 The Principal retains a list of those parents/carers who have objected to or who have placed any restrictions or limitations on the use of images of their child.

16.4 **Staff should familiarise themselves with the names of the students on that list. It is a disciplinary offence to use, post or publish a photograph or video image of a student contrary to the instructions of their parent/carer.**

17. Exam results

We will ensure that students and their parent/carers are notified of our intention to publish exam results, the method by which they will be published and the format of the intended publication in advance of their publication and we will reasonably consider a data subject's objection to the publication of their exam results.

18. Changes to this policy

We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.

Appendix A: Third parties with whom the School shares data - 2016

Organisation	Reason for sharing	Information shared
Parentpay	To facilitate payments into school for trips, events and other purchases	Student name, DOB, Gender, school admission number, Unique Pupil Number, registration group, year group, parent name, address, telephone number, meal arrangements, eligibility for free school meals, ethnicity, religion, dietary needs, meal pattern Payments secured by Payment Card Industry Data Security Standard (PCIDSS)
GCSEPod	GCSE revision website. By sharing data, PCSA is able to track how often students are accessing the revision materials and which topics are being studied	Student name, Unique Pupil Number, student e-mail address, DOB, gender, year group
Contact Group (Truancy Call/Parent Call)	Truancy Call is our absence call line for automated calls to parents if students not in school. Parent Call is used for reminders about parents evenings, Books4U and can be used in emergencies such as school closures	Student name, DOB, gender, school admission number, registration group, ethnicity, religion, parent(s) name(s), parent(s) phone number(s), parent(s) e-mail(s)
My Maths	Maths revision site	Student name, maths class
Weston College/Bridgwater College (Year 11 only)	To ensure that Year 11 students have full information available to them during the transition to sixth form education	Student name, DOB, gender, address
Colorfoto	To facilitate the distribution of school photographs and the import of photographs onto the school Sims system	Student name, registration group, school admission number
Kerboodle (Years 7 and 8 only)	Science homework/resources website	Student name, registration group, science class
Aspens Caterers	Provision of free school meals	For students currently

	to appropriate students	eligible for free school meals only: Student name, registration group
Accelerated Reader (Years 7 and 8 only) (Hosted by Renaissance Learning)	Reading programme used to track students' progress in reading related to their chronological age	Student name, DOB, English class.
PiXL Maths App	Maths revision and practice questions	Student name, year group, maths class. Students will be asked to enter an e-mail address when they first register for password reminders. Use of school e-mail address will be recommended.