



DATA PROTECTION POLICY

| Issue No | Author/ Owner | Date Written | Approved by Governors on | Comments |
|----------|------------------|-----------------|-----------------------------|------------|
| 1 | PC | November 2014 | 11 March 2015 | |
| 2 | PC | November 2016 | 22 February 2017 | No changes |

1 General Statement

Backwell School collects and uses personal information about staff, students, parents and other individuals to enable it to provide high quality education and comply with its statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are available on the ICO's website. Schools also have a duty to issue a Fair Processing Notice to all students/parents and staff, this summarises the information held, why it is held and the other parties to whom it may be passed on.

2 Purpose

This policy is intended to ensure that personal information is dealt with correctly, securely and in accordance with the Data Protection Act 1998, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

3 What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

4 Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

- (i) Personal data shall be processed fairly and lawfully;
- (ii) Personal data shall be obtained only for specified and lawful purposes;
- (iii) Personal data shall be adequate, relevant and not excessive;
- (iv) Personal data shall be accurate and where necessary, kept up to date;

- (v) Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
- (vi) Personal data shall be processed in accordance with the rights of those individuals to which the data relates under the Data Protection Act 1998;
- (vii) Personal data shall be kept secure i.e. protected by an appropriate degree of security (see Appendix 1, Note 1);
- (viii) Personal data shall not be transferred to a country or territory outside the European Union, unless that country or territory ensures an adequate level of data protection.

5 Policy Statement

The school is committed to maintaining the above principles at all times. Therefore the school will issue students/parents and staff with a Fair Processing Notice detailing:

- Why and when the information is being collected.
- When, why and with whom their information might be shared.

The school will ensure that it:

- Checks the quality and the accuracy of the information it holds.
- Ensures that information is not retained for longer than is necessary.
- Ensures that when obsolete, information is appropriately and securely destroyed.
- Ensures that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Shares information with others only when it is legally appropriate to do so.
- Sets out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests (See Appendix 1, Note 2).
- Ensures our staff are aware of and understand our policies and procedures.

6 Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

7 Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every two years. The policy review will be undertaken by the Governing Body.

8 Contacts

If you have any enquires in relation to this policy, please contact the Headteacher who will also act as the contact point for any access requests.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 5457453

Note 1: Procedures at school for keeping personal data safe and secure

- 1 Staff should never disclose their username and password to anyone and should ensure they are properly logged off at the end of every session.
- 2 Secure, remote access is provided to staff in order to avoid taking personal data off site. Staff who make use of the secure remote access facility should not connect to it over an unsecured home wireless network. WPA is an expected minimum encryption standard for wireless communication but, preferably a hard-wired connection will be used.
- 3 Up to date virus and malware checking software will be used on every computer device on the School Network.
- 4 Staff will be given enough access to SIMS (our school management and information system) to enable them to discharge the responsibilities of their post, but not anything more excessive.
- 5 Staff must ensure that computers and laptops are locked (ctrl + alt + del or windows key + L) when not in use.
- 6 Personal data that is allowed to be shared with third parties will be sent out in the post marked confidential or the School will make use of the secure government data transfer website if applicable. Personal data required for governors to fulfil their role must either be sent as hard copy in the post or uploaded to the secure governors' portal. Personal data will not be sent out by email.

Note 2: Procedures for responding to access requests made under the Data Protection Act 1998

- 1 Requests for information must be made in writing; which includes email, and be addressed to the Headteacher. If the initial request does not clearly identify the information required, then further enquiries will be made.
- 2 The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:
 - Passport
 - Driving licence
 - Utility bills with the current address
 - Birth / Marriage certificate
 - P45/P60
 - Credit Card or Mortgage statement

This list is not exhaustive.

- 3 Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to

consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

- 4 The school may make a charge for the provision of information, dependent upon the following:
 - If the information requested is only the educational record, viewing will be free, but a charge not exceeding the cost of copying the information will be made by the School.
 - Should the information requested be personal information that does not include any information contained within educational records the schools will charge £10 to provide it.
- 5 The response time for subject access requests, once officially received, is 40 days (**not working or school days but calendar days, irrespective of school holiday periods**). However the 40 days will not commence until after receipt of fees or clarification of information sought.
- 6 The Data Protection Act 1998 allows exemptions as to the provision of some information; **therefore all information will be reviewed prior to disclosure.**
- 7 Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40 day statutory timescale.
- 8 Any information which may cause serious harm to the physical or mental health or emotional condition of the child or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.
- 9 If there are concerns over the disclosure of information then additional advice should be sought.
- 10 Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.
- 11 Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.
- 12 Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

This policy should be read in conjunction with the ICT Acceptable Use Policy and the Data Protection Policy.