

# Whitecross Hereford: High School & Specialist Sports College

Policy: Data Protection

Reviewed by: Staff and Finance Committee

Reviewed on: 13 June 2016

Approved by Full Board

Related documents: Publication of Information Scheme (Staff & Finance Committee)  
Information Sharing Protocol (PDB&W Committee)  
Safeguarding & Child Protection Policy (PDB&W C'ttee)  
Record Retention Schedule (Business Manager)  
CCTV Code of Practice (Business Manager)  
IRIS classroom observation protocol (Deputy Headteacher)  
ICT User Agreement Form (Staff & Student)

Whitecross Hereford is required to process relevant personal data regarding staff, students and their parents/guardians/carers and will take all reasonable steps to do this in accordance with this policy and related school documents. Processing may include obtaining, recording and holding, disclosing, destroying or otherwise using data. Reference to students and staff in this policy includes current, past and prospective.

The school is registered with the Information Commissioner's Office (ICO) and is entered on the Data Protection Register (Z5588982). Details are retained in the Business Manager's Office.

Data protection procedures will be followed by all staff members and as far as is reasonably practicable will comply with the principles of the Data Protection Act (DPA) 1998 to ensure all personal data is:

- Fairly and lawfully processed;
- Only processed for specified purposes;
- Adequate, relevant and not excessive;
- Accurate and kept up to date;
- Not kept for longer than necessary;
- Processed in accordance with the individual's legal data rights;
- Securely protected against unauthorised processing, accidental loss, destruction or damage;
- Not transferred outside the EEA without adequate protection.

Definitions of data are highly complex and difficult to define categorically, however within the context of Whitecross Hereford it is suggested that 'personal data' may include:

- School admission and attendance data;
- Students curricular records;
- Students assessment reports to parents;
- Students exam entry details and results;
- Staff records including payroll details;
- Student and staff disciplinary records;
- Teacher's professional record data;
- Records of contractors or suppliers.

If it is necessary for the school to process certain data to fulfil its obligations to students and their parents/guardians/carers, then consent is not required. However, any information which falls under the definition of personal data and not otherwise exempt (e.g. the prevention of detection of crime or the assessment of any tax or duty) will remain confidential and will only be disclosed to third parties with the consent of the appropriate individual or under the terms of this policy.

Sensitive personal data, such as detailed below, may be processed by the school but with the explicit consent of the appropriate individual given in writing:

- Ethnic or racial origin;
- Political opinions;
- Religious or other similar beliefs;
- Membership of a trade union;
- Physical or mental health/condition;
- Sexual life;
- Offence or alleged offence;
- Proceedings or court sentence.

Individuals have a right, under the 1998 Act to access the information held by the school. Any request should be put in writing to the Headteacher who will respond as soon as is reasonably practicable and in any event, within 21 days for access to information and within 40 days for access to records.

Parents/guardians/carers should make any request for information regarding their child's educational record to the Governing Body via the Headteacher.

Data which is exempt from a right of access under the DPA, includes:

- Information which identifies other individuals;
- Information which the school reasonably believes is likely to cause damage or distress;
- Information which is subject to legal professional privilege;
- Student examination scripts.

The school will also treat as confidential any reference given for the purpose of education, training or employment of any student. The school acknowledges that an individual may have the right to access a reference relating to them received by the school, but this would only be disclosed if doing so does not identify the referee.

Under the DPA, the rights to data belong to the individual to whom the data relates. However in most cases the school will rely on parental consent to process data relating to the student unless, given the circumstances and the student's age and understanding, it is unreasonable to do so.

Where a student seeks to raise private concerns confidentially with a member of staff and makes it clear that they do not want the data passed on to their parents/guardians, the school will maintain confidentiality unless it has reasonable grounds to believe that the student does not fully understand the consequences of withholding their consent or where the school believes the disclosure will be in the best interest of the student or other persons.

The school will not generally disclose information about individuals without consent, however for the following purposes the school does intend to disclose data as is necessary to third parties:

- To give confidential references to educational institutions that the student may wish to attend;
- To publish the results of public examinations or other achievements of students;
- To disclose medical details for the purposes of school trips, etc.

As part of the entry procedure into the school at any age, parents/guardians are asked to complete and sign a Confidential Information form which includes giving consent, or otherwise, to use photographic images or video clips in school related publications and school website and any other marketing materials. It also enables parents to consent, or otherwise, for their child to be registered on the school's biometric cashless catering system.

The school will ensure that:

- as far as reasonably practicable, that all personal data is accurate and up to date;
- all staff are made aware of this policy and its related documents;
- all personal data is held in secure, central locations and is not accessible to unauthorised persons;
- procedures and protocols for the safe and confidential disposal of sensitive data will be implemented and adhered to.