Data Protection and Handling Policy

This policy is in line with the Ethos and Values of Blackburn Central High School with Crosshill

Document Control

This policy has been approved for operation within Blackburn Central High School and Crosshill School

Date approved	October 2017
Approved by	Finance & Resources
Date of next review	October 2019
Review period	2 Years
Policy status	Statutory
Owner	CSI

Headteacher
Mrs. D Atkinson
Haslingden Road
Blackburn BB2 3HJ
tel. 01254 505 700
fax. 01254 505 701
eml. info@bchs.co.uk
web. www.bchs.co.uk
@BCHS_uk
BCHS with Crosshill

Data Protection and Handling Policy

Blackburn Central High School with Crosshill uses personal information to educate our students and fulfil our statutory obligations. We take data protection very seriously and all members of staff will do everything in their power to keep personal information secure.

Anyone with access to personal data must follow our data protection policy. The policy combines requirements from data protection legislation with other relevant guidance. Members of staff who handle personal data should familiarise themselves with these regulations as well as the school's policy.

Personal Data

The Data Protection Act defines "Personal Data" as data relating to a living individual who can be identified from those data or from other information held by, or likely to come into the possession of, the data controller.

The school holds a range of personal data (including personal information about members of the school community, professional records of staff members and academic information) in digital form and as paper records.

Data Protection Principles

Under the Data Protection Act 1998, data controllers must adhere to the following eight principles. Personal data should be:

1. Processed fairly and lawfully.
2. Obtained only for one or more specified and lawful purposes.
3. Adequate, relevant and not excessive.
4. Accurate and kept up to date where necessary.
5. Kept for no longer than is necessary for that purpose or those purposes.
6. Processed in accordance with the rights of data subjects under the Data Protection Act 1998.
7. Protected by an appropriate degree of security.
8. Transferred only to countries with adequate security and data protection measures.

Training

All staff will receive training in data protection and handling. They will be made aware of their responsibilities as outlined in this policy through induction and training procedures.

General Statement

We are fully committed to upholding the above principles and will:

- Inform individuals why personal information is collected.
- Notify individuals when their data is shared and explain why and with whom it was shared.
- Maintain the quality and accuracy of personal data.
- Not retain information for longer than necessary.
- Destroy any information that is no longer needed appropriately and securely.
- Protect all personal information from loss, theft and unauthorised disclosure.
- Share information with others only when legally appropriate.
- Set out procedures to ensure compliance with Subject Access Requests.
- Make sure all staff are fully aware of our policies.

Responsibilities

The school's Senior Information Risk Officer (or SIRO) is Nicola Chester/Business Manager (NChester618@bchs.co.uk). The SIRO will keep up to date with relevant guidance and legislation and will:

- Take responsibility for the school's information risk policy and risk assessment.
- Appoint the Information Asset Owners (or IAOs).

The school will identify Information Asset Owners (IAOs) for student information, staff information and any other types of data being held. IAOs will manage risks to the information and will know:

- What information is held, for what purpose and for how long.
- How information is amended or added to over time.
- Who has access to protected data and why.

In addition to the specific responsibilities outlined above, everyone in the school must handle personal data with care and sensitivity. This includes school governors if they have access to personal information in the course of their roles.

Registration

We are registered as a data controller on the Data Protection Register held by the Information Commissioner. The register can be searched here.

'Fair Processing Notice' – Information for Parents and Carers

In compliance with the fair processing requirements of the Data Protection Act, we keep parents and carers informed about the student data we collect, the purposes for which it is held and any third parties with whom it may be shared. This fair processing notice (commonly referred to as a privacy notice) is available via the school website, staff handbook and on other key documentation which will be shared before or as soon as personal information is collected.

Storage and Access

Our ICT systems include security measures to prevent unauthorised users from accessing protected files. All users are assigned a role and clearance which will determine their access to protected data.

Users must set strong passwords, change them regularly, and never share them. Personal data will only be accessed from password protected devices which should be locked when not in use. We will take appropriate steps to keep data storage media physically secure.

Removable media (including USB sticks, mobile devices, etc.) should NOT be used to store personal data. The school is aware that data storage in remote and cloud storage systems (like Dropbox and Google Drive) must also comply with the Data Protection Act. Our policies on cloud-based storage are in line with ICO guidance and we ensure that we are satisfied with the security offered by remote/cloud based service providers before using them.

Subject Access Requests

Data subjects have a number of rights under Section 7 of the Data Protection Act, including the right of access. Any Subject Access Requests (written requests made by a data subject to see all or some of the personal data held by the data controller) will be dealt with according to the school's procedures as follows:

Data subjects may request:

- To know if the school holds personal information about them
- A description of any data held
- The purpose for which the data is processed
- The sources of the data
- To whom the data may be disclosed
- A copy of all their personal data.

Under some circumstances data subjects may have additional rights related to blocking, destruction and rectification of data.

Data Transfers and Remote Access

It may sometimes be necessary to transfer personal data to the local authority or other agencies, or for members of staff to access personal information outside of school. In these cases:

- Users must have permission to access or transfer the data out of school and use appropriately secured media/devices
- Devices containing personal data may only be accessed by authorised users
- Where possible, personal data should be accessed via secure remote access to the school's management information system (i.e. via Citrix)
- Users should securely store and protect any personal devices used to access data.

BwD local authority should be consulted if it is necessary to transfer data to another country.

Disposal

Disposal of personal data that is no longer needed should make reconstruction highly unlikely. We dispose of all personal data in compliance with the requirements for safe destruction. We overwrite files, shred and incinerate media and dispose of all other information in accordance with relevant government guidance.

The school's Destruction Log should be used to record the disposal of all personal information. Further, these records should contain:

- The document ID
- Classification
- Authorisation
- Date and method of destruction