Cribden House School - General Data Protection Regulation

Our Commitment:
Cribden House School is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and Data Handler under the General Data Protection Regulation (GDPR) May 2018.

The legal basis for processing data are as follows –

- **Contract**: the processing is necessary for the member of staff's employment contract or student placement contract.
- **Legal obligation**: the processing is necessary for the school to comply with the law (not including contractual obligations)

All members of staff responsible for data protection within school, which is overseen by our Data Protection Officer – Vicky Ward and overall Data Controller Head Teacher – Siobhan Halligan.

As Data Controllers and handlers, we are committed to ensuring that staff are aware of all data protection policies, legal requirements and adequate training is provided to them to ensure all act in accordance with GDPR rules.

The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

Notification:
Our data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller.

Details are available from the ICO:
https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO.

Personal and Sensitive Data:
All data within the school's control shall be identified as personal, sensitive or both.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/

The principles of the General Data Protection Act shall be applied to all data processed:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Fair Processing / Privacy Notice:

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual's data.

There may be circumstances where the school is required either by law or in the best interests of our pupils or staff to pass information onto external authorities, for example local authorities, Ofsted, or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect. The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information. Any proposed change to the processing of individual's data shall first be notified to them. Under no circumstances will the school disclose information or data:

- that would cause serious harm to the child or anyone else's physical or mental health or condition
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- recorded by the pupil in an examination.
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed
- in the form of a reference given to another school or any other place of education and training, the child's potential employer, or any national body concerned with student admissions.

Data Security:
How data/information is processed and the impact on the individual's privacy throughout these activities have been assessed for potential risk. Risk and impact assessments shall be conducted in accordance with guidance given by the ICO.

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data.

Data Access Requests (Subject Access Requests):
All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and they should be made in writing to:

No charge will be applied to process the request.

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child.

Data may be disclosed to the following third parties without consent:

• Other schools – where the pupil is transferring out to another school permanently.

• Examination authorities - where the pupil is sitting an exam set by an external body.

• Health authorities - As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

• Police and courts - where a criminal investigation arises information may be forwarded on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

• Social workers and support agencies - to protect or maintain the welfare of our pupils, personal data/information may need to be shared with social workers or support agencies.

• Educational division - data sharing to aid the government in monitoring the national educational system and enforcing educational laws.

• Right to be Forgotten - where personal data is no longer required for its original purpose, individuals can demand processing is stopped and all personal data is erased including any data held by contracted processors.

Photographs and Video:
Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school.

Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources.

It is the school's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent.

Location of information and data:
Hard copy data, records, and personal information are stored out of sight and in a locked cupboard.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Sensitive or personal information and data should not be removed from the school site, unless required for offsite meetings, school visits with pupils or where emergency contact details are required on school trips. Any information removed from school should be kept safe and out of sight of any third party, it should be returned to school and destroyed on the school premises if no longer required.

- Obsolete data, sensitive information or pupil files should be shredded in accordance with the retention policy. This applies to handwritten notes, where reference is made to a pupil or staff member.

- No sensitive/personal information should be left accessible and should be cleared away when not in use and locked away.

- PC's/Laptops/Ipads being used to work with sensitive information should be locked when not in use with an undisclosed password.

- To access school information from home, only Remote Assess supplied by our ICT department should be used.

- USB sticks/disks should not be used under any circumstances.

Data Disposal:
The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data in any form will be destroyed in line with the ICO Retention document.

Disposal of IT assets holding data shall follow ICO guidance.

The school uses our own shredder to dispose of sensitive data that is no longer required. This is not contracted out to a third party.

Date of Policy Implementation: **May 2018**
Updated: July 2022
Date of Next Review: **July 2023**