The Governing Body for Carisbrooke College and Medina College

DATA PROTECTION POLICY

Date Adopted:	May 2018
Revision date(s):	
Release / circulation date(s):	
Date of next review:	May 2019

The General Data Protection Regulation (GDPR) replaces the Data Protection Act and came into effect on 25th May 2018. The data protection laws needed to change because the old ones were out of date in today's digital world. The GDPR was created to strengthen data protection for people within the EU. It aims to give individuals more control over their personal data and make it easier for them to access.

Medina College is the data controller for the personal information you provide. Medina's Data Protection Officer is the Head of Legal Services and Monitoring Officer and can be contacted at dpo@iow.gov.uk.

Your information will be used to enable us to provide an education for your child. Your data may be shared with the local authority, department for education and other third parties if we are required to do so by law. We will retain your details until your child reaches the age of 25 (or 30 for students with a statement/Education Health Care Plan). You can review any of our policies including our retention policy and full privacy notice on our website. For further details on how your information is used; how we maintain the security of your information; and your rights including how to access information we hold on you, and how to complain if you have any concerns about how your personal details are processed, please visit our website or email info@carisbrooke.iow.sch.uk or call main reception on 01983 524651

The Governing body for Carisbrooke College and Medina College (which include the co-located sixth forms on the VI Form Campus) collect and use personal information (referred to in the Data Protection Act as personal data) about staff, students, parents and other individuals who come into contact with the schools. This information is gathered in order to enable the provision of education and other associated functions. In addition, the schools may be required by law to collect, use and share certain information.

The schools are each registered as a Data Controller with the Information Commissioner's Office (ICO) and have appointed an Isle of Wight Local Authority based Data Protection Officer **Helen Miles and her team** to inform advise and monitor each school's compliance with the new General Data Protection Regulation (GDPR). Full details of which are available on the ICO website: https://ico.org.uk/.

The schools issue a Privacy Notice to all students/parents which summarises the information held on students, why it is held and the other organisations to whom information may be passed to.

Purpose

This policy sets out how the schools deal with personal information correctly and securely and in accordance with the GDPR, Data Protection Act, and other related legislation.

This policy applies to all personal information however it is collected, used, recorded and stored and whether it is held on paper or electronically.

All school staff and governors involved with the collection, use, processing or disclosure of personal data will be aware of their duties and responsibilities and will adhere to this policy.

What is Personal Information/Data?

Personal information or data is information which relates to a living individual who can be identified from that data, or from the data in addition to other information available to them.

Personal data includes (but is not limited to) an individual's name, address, date of birth, photograph, bank details and other information that identifies them.

What is Sensitive Personal Data?
Sensitive personal data (referred to in the GDPR as "special categories of personal data") includes information as to an individual's racial or ethnic origin, their political opinions, religious beliefs or beliefs of a similar nature, whether they are a member of a trade union, their physical or mental health or condition, sexual life, the commission or alleged commission of an offence and any proceedings for an offence committed or alleged to have been committed by them, the disposal of those proceedings or the sentence of any court in such proceedings.

Data Protection Principles
In accordance to the requirement outlined in the GDPR personal data will be:

1. Processed fairly, lawfully and in a transparent manner in relation to individuals.
2. 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 or statistical purposes shall not be considered to be incompatible with the initial purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regards for the purposes for which they are processed, are erased and rectified without delay.
5. Kept in a form which permits identification of data subjects for longer than 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 purposed 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.
6. Processed in a manner that ensures appropriate security if the personal data, including protection against unauthorised or unlawful processing and against accidental lost, destruction or damage, using appropriate technical or organisational measures.

Accountability
In accordance to the requirement outlined in the GDPR each school will:

7. Implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.
8. Provide comprehensive, clear and transparent privacy policies.
9. Maintain clear records of activities relating to higher risk processing, such as the processing of special categories of data o that in relation to criminal convictions and offences.
10. Ensure internal records of processing activities will include the following:
    - Name and details of organisation
    - Purpose(s) of the processing
    - Description of the categories of individuals and personal data
    - Retention schedules
    - Categories of recipients by personal data
    - Description of technical and organisational security measures
    - Details of transfers to third world countries, including documentation of the transfer mechanism safeguards in place *(not applicable)*

11. Implement measure that meet the principles of data protection by design and data protection by default such as:
    - Data minimisation
    - Pseudonymisation
    - Transparency
    - Allowing individuals to monitor processing
    - Continuously creating and improving security features
12. Data protection impact assessments will be used, where appropriate

Commitment

The Governing Body is committed to maintaining the above principles at all times. Therefore the schools will:

- Inform individuals why personal information is being collected.
- Inform individuals when their information is shared, and why and with whom unless the GDPR or Data Protection Act provides a reason not to do this.
- Obtain consent before processing Sensitive Personal Data, even if consent is implied within a relevant privacy notice, unless one of the other conditions for processing in the Data Protection Act applies.
- Check the accuracy of the information it holds and review it at regular intervals.
- Ensure that any inaccurate or incomplete personal data is rectified within the correct timeframe.
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorized disclosure, irrespective of the format in which it is recorded.
- Ensure that personal information is not retained longer than it is needed.
- Ensure that when information is destroyed that it is done so appropriately and securely.
- Share personal information with others only when it is legally appropriate to do so.
- Comply with the duty to respond to requests for access to personal information, known as Subject Access Requests.
- Ensure that personal information is not transferred outside the EEA without appropriate safeguards.
- Ensure that staff are aware of what constitutes a data breach and any data breaches are dealt with using the correct procedure and in a timely fashion.
- Ensure all staff and governors are aware of and understand these policies and procedures.

Complaints

Complaints will be dealt with in accordance with the schools' complaints procedures which can be found on the websites. Copies can also be obtained from the schools. Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF or at www.ico.gov.uk.

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every three years. The policy review will be undertaken by the governing body for Carisbrooke College and Medina College.

Contacts

If you have any enquires in relation to this policy, please contact the respective Data Officer for Carisbrooke College or Medina College as appropriate who will also act as the contact point for

any subject access requests.