Castle Donington College

Data Protection Policy 2019

Date adopted Full Governing Board **9th December 2019**

Date for review **December 2020**

Signed by Chair of Governors

This College follows Guidance and Advice given by the Government when writing policies; in light of this, changes may need to be made after the adoption of this policy and prior to the review date.

Policy Statement

This policy applies to all employees and agents of Castle Donington College, and to contractors, suppliers and consultants employed by the College, insofar as they may collect, hold, access or dispose of personal data relating to the business of the College.

The provisions of this policy extend to personal data held on any personal computers or person organisers, or in the structured manual files, even if not owned by Castle Donington College, when used by members of staff, or external contractors and advisors, specifically to support the business activities of the College (e.g. use of laptops or home PCs by staff for business purposes).

Any breach of Data Protection Act of 2018 or the Castle Donington Data Protection Policy will be considered misconduct and, in the event, the College Disciplinary Procedure will be applied.

Responsibility and Implementation

It is the responsibility of all employees to adhere to this policy. The implementation of this policy on an operation level is the responsibility of the Senior Leadership Team (SLT).

It is the responsibility of all staff to ensure that College records are as accurate and up-to-date as possible, ensuring changes to personal data are promptly reported to SLT to allow the College Management Information System (Sims.net), to be maintained at all times.

Introduction

The College collects and uses certain types of personal information (data) about staff, pupils, parents and other individuals who come into contact with the College in order to provide learning and teaching and other functions. In addition it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities, government agencies and other bodies.

This policy is intended to ensure that personal information must be dealt with properly and securely and in accordance with the Data Protection Acts 2018 plus any subsequent amendments and other related legislation. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Castle Donington College Commitment

The College is committed to maintaining the data protection principles at all times. This means that the College will:

- Tell you what purposes we will use information for when we collect it
- If information will be shared we will tell you why, which whom and under what circumstances
- Check the quality and accuracy of the information we hold
- Apply our Retention Policy to ensure that information is not held longer than is necessary
- Ensure that when information is authorised for disposal it is done appropriately
- Ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system
- Share personal information with others only when it is necessary and legally appropriate to do so
- Set out clear procedures for responding to requests for access to personal information
- Train our staff so that they are aware of our policies and procedures

The **Data Protection Act 2018** controls how personal information is used by organisations, businesses or the government. The **Data Protection Act 2018** is the UK's implementation of the General **Data Protection** Regulation (GDPR).

What is the GDPR?

This is a European Directive that was brought into UK law with an updated Data Protection Act 2018.

What is the point of the GDPR?

The GDPR and new DPA exist to look after individual's data. It is a series of safeguards for every individual. Information about individuals needs to be treated with respect and be secure.

The GDPR exists to protect individual rights in an increasingly digital world.

Who does it apply to?

Everyone, including schools. As public bodies, schools have more obligations than some small businesses. It is mandatory to comply with the GDPR and proposed provisions in the new Act.

Castle Donington College wants to make sure information about pupils, parents, staff and volunteers is kept secure and within the law.

What is Data?

Any information that relates to a living person that identified them. This can be by name, address or phone number for example. It also relates to details about that person, which can include opinions.

Some data is considered to be more sensitive, and therefore more important to protect. This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.

Schools often collect sensitive data for DfE and LA requirements and of course pupil data may contain information about safeguarding, SEN or health needs. Information about other family members may also be on the school file.

Every school also has to publish a Privacy / Fair Processing Notice on the website.

What are the key principles of the GDPR? Lawfulness, transparency and fairness.

School must have a legitimate reason to hold the data, we explain this in the Data Privacy Notices on the website. The College will ask for consent to use data about a pupil for a particular purpose. If you wish to withdraw consent, there is a form to complete to allow us to process your request. There are occasions when you cannot withdraw consent as explained in 'Data Subjects Rights'.

Collect data for a specific purpose and use it for that purpose

Data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

Limited collection

Data controllers should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack only limited information can be lost.

Accuracy

Data collected should be accurate, and steps should be taken to check and confirm accuracy. The College does this when pupils join the school and check on an annual basis.

If a Data Subject feels that the information held is inaccurate, should no longer be held by the Controller or should not be held by the Controller in any event a dispute resolution process and complaint process can be accessed, using the suitable forms.

Retention

Castle Donington College has a Retention Policy that explains how long we store records for.

Security

We have processes in place to keep data safe. That might be paper files, electronic records or other information.

Who is a 'data subject' ?

Someone whose details we keep on file. Some details are more sensitive than others. The GDPR sets out collection of details such as health conditions and ethnicity which are more sensitive than names and phone numbers.

Data subjects' rights

Individuals have a right:-

- to be informed
- of access to data stored about them or their children
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for school to keep the data
- to restrict processing, i.e. to limit what is done with their data
- to object to data being shared or collected

There are other rights that relate to automated decision making and data portability that are not directly relevant in schools.

Data subjects rights are also subject to child protection and safeguarding concerns, sharing information for the prevention and detection of crime. Schools also have legal and contractual obligations to share information with organisations such as the Department for Education, Social Care, the Local Authority and HMRC amongst others. In some cases these obligations override individual rights.

Subject Access Requests

Copies of information that we hold about a parent/carer or a pupil can be requested. This Subject Access Request process is set out separately. A form will need to be completed and identification evidence will be required for the College to process the request.

The College has a month to provide the information, but this can be extended if, for example, the College was closed for holidays. The maximum extension is up to two months.

The College may require the request to be specific about the information that is required. This is to ensure that the information provided is relevant to the query.

There may be some cases where all information cannot be given if there are contractual, legal or regulatory reasons.

The College cannot release information provided by a third party without their consent.

The College will supply the information in an electronic form.

Who is a 'data controller'?

Our College Governing Board is the Data Controller. They have ultimate responsibility for how the College manages data. They delegate this to Data Processors to act on their behalf.

Who is a 'data processor'?

This is a person or organisation that uses, collects, accesses or amends the data that the controller has collected or authorised to be collected. It can be a member of staff, a third-party company, possibly a governor, a contractor or temporary employee. It can also be another organisation such as the police or the LA.

Data controllers must make sure that Data Processors are as careful about the data as the controller themselves. The GDPR places additional obligations on organisations to make sure that Data Controllers require contractual agreements to ensure that this is the case.

Processing data

The College must have a reason to process the data about an individual. Our privacy notices set out how the College uses data. The GDPR has 6 conditions for lawful processing and any time the College processes data relating to an individual it is within one of those conditions.

If there is a data breach there is procedure to follow to take immediate action to remedy the situation as quickly as possible.

The legal basis and authority for collecting and processing data in College are:-

- consent obtained from the data subject or their parent
- performance of a contract where the data subject is a party
- compliance with a legal obligation
- to protect the vital interests of the data subject or other associated person
- to carry out the processing that is in the public interest and/or official authority
- it is necessary for the legitimate interests of the data controller or third party
- in accordance with national law.

In addition, any special categories of personal data are processed on the grounds of

- explicit consent from the data subject or about their child
- necessary to comply with employment rights or obligations

- protection of the vital interests of the data subject or associated person
- being necessary to comply with the legitimate activities of the school
- existing personal data that has been made public by the data subject and is no longer confidential
- bringing or defending legal claims
- safeguarding
- national laws in terms of processing genetic, biometric or health data
- processing data is recorded in College.

Data Sharing

Data sharing is done within the limits set by the GDPR. Guidance from the Department for Education, health, the police, local authorities and other specialist organisations may be used to determine whether data is shared.

The basis for sharing or not sharing data is recorded in College.

Breaches & Non Compliance

If there is non compliance with the policy or processes, or there is a DPA breach as described within the GDPR and DPA 2018 then the guidance set out in the Breach & Non Compliance Procedure and Process needs to be followed.

Protecting data and maintaining data subject's rights is the purpose of this policy and associated procedures.

Consent

The College will seek consent from staff, volunteers, pupils, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required.

Consent is defined by the GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

The College may seek consent from pupils also, and this will be dependent on the child and the reason for processing.

Consent and Renewal

On the College website there are 'Privacy Notices' that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail.

Obtaining clear consent and ensuring that the consent remains in place and that the information held is accurate, is important for the College.

For Pupils and Parents/Carers

When a pupil enrolls at the College, parents/carers will be asked to complete a form giving next of kin details, emergency contact and other essential information. Consent will be sought to use the information for other in College purposes, as set out on the data collection/consent form. It is important to inform school if details or decisions about consent changes. A form is available.

Pupil Consent Procedure

Where processing relates to a child under 16 years old, the College will obtain the consent from a person who has parental responsibility for the child.

Pupils may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent the school will consider each situation on the merits and within the principles of GDPR and also child welfare, protection and safeguarding principles.

Please complete the appropriate form.

CCTV

We use CCTV and store images for a period of time in line with the policy. CCTV may be used for:-

- detection and prevention of crime
- College staff disciplinary procedures
- pupil behaviour and exclusion management processes
- to assist the College in complying with legal and regulatory obligations

Data Protection Officer

The College's Data Protection Officer, is John Walker, Solicitors. 14 Forsells End, Houghton on the Hill, LE7 9HAQ.

Their role is to:-

- to inform and advise the controller or the processor and the employees who carry out

processing of their obligations under the GDPR
- to monitor compliance with the GDPR and DPA
- to provide advice where requested about the data protection impact assessment and monitor its performance
- to be the point of contact for Data Subjects if there are concerns about data protection
- to cooperate with the supervisory authority and manage the breach procedure
- to advise about training and CPD for the GDPR

Physical Security

In College, every secure area has individuals who are responsible for ensuring that the space is securely maintained and controlled if unoccupied, i.e. locked. Offices and cupboards that contain personal data should be secured if the processor is not present.

The Premises Manager is responsible for authorising access to secure areas along with SLT/Business Manager.

All staff, contractors and third parties who have control over lockable areas must take due care to prevent data breaches.

Secure Disposal

When disposal of items is necessary a suitable process must be used. This is to secure the data, to provide a process that does not enable data to be shared in error, by malicious or criminal intent.

These processes, when undertaken by a third party are subject to contractual conditions to ensure GDRP and DPA compliance.

Complaints & the Information Commissioner Office (ICO)

The Complaints Policy deals with complaints about Data protection issues.

There is a right to complain if parent/carers feel that data has been shared without consent or lawful authority.

A complaint can be made a request has been made to erase, rectify, not process data and the College has not agreed to your request.

The College will always try to resolve issues on an informal basis, and then through our formal complaints procedure. Please complete the form, and the College will make contact with more details about the timescale and process.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations. Email: casework@ico.org.uk
Helpline: 0303 123 1113 web: www.ico.org.uk

Review

A review of the effectiveness of GDPR compliance and processes will be conducted by the Data Protection Officer annually.