



Calday Grange
Grammar School

DATA PROTECTION POLICY

January 2016

Approved by Full Governing Body: 11th February 2016

DATA PROTECTION POLICY

Contents:

- Statement of intent
- Data controller and responsibilities
- Staff responsibilities
- Data security
- Subject consent
- Rights to access information
- Publication of information
- Data retention
- Challenges and compensation

Statement of intent

Calday Grange Grammar School is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the Data Protection Act 1998.

This policy will outline how the school will comply with the key principles of the Data Protection Act:

- Data must be processed fairly and lawfully.
- Data must only be acquired for one or more lawful purposes and should not be processed for other reasons.
- Data must be adequate, relevant and not excessive.
- Data must be kept accurate and up-to-date.
- Data must not be kept for longer than is necessary.
- Data must be processed in accordance with the data subject's rights.
- Appropriate measures must be taken to prevent unauthorised or unlawful access to the data and against loss, destruction or damage to data.
- Data must not be transferred to a country or territory unless it ensures an adequate level of protection for the rights of the subject.

Data controller and responsibilities

The school as the corporate body is the Data Controller.

The governing body of Calday Grange Grammar School therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

The School holds and maintains different types of data; across the school various staff have responsibility for its security and access arrangements:

The Senior Information Risk Officer (SIRO) at Calday Grange Grammar School is the Headteacher who has the following responsibilities:

- They own the information risk and regularly review the risk register
- They delegate responsibility for maintenance, security of and training of data protection to Information Asset Owners (IAOs)*
- They act as an advocate for information risk management

** Includes posts such as: Director of Finance & Operations, Director of Student Services, Deputy Headteachers, Directors, ICT Network Manager plus other relevant posts.*

The Information Asset Owners (IAOs) will know:

- What information is held and for what purposes
- How information will be amended or added to over time
- Who has access to data and why
- How information is retained and disposed of

The Director of Finance & Operations will deal with the day-to-day matters relating to data protection.

Staff responsibilities

Calday Grange Grammar School recognises that its staff members and pupils need to know what the school does with the information it holds about them.

All staff members, including members of the school governing body will receive training in their responsibilities under the Data Protection Act as part of their induction and through additional training sessions

Parents will receive a copy of the Privacy Notice upon registration of their child at Calday Grange Grammar School which includes an overview of the information that the school will keep about their child.

Staff members and parents are responsible for checking that any information that they provide to the school in connection with their employment or in regard to a registered pupil is accurate and up-to-date.

The school cannot be held accountable for any errors unless the employee or parent has informed the school about such changes.

Data security

Staff members of Calday Grange Grammar School will ensure that personal data is secured in accordance with the provisions of the Data Protection Act by:

- Keeping the data in a locked filing cabinet, drawer or safe.
- Ensuring that computerised data is coded, encrypted or password protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
- Where data is saved on removable storage, holding the storage device in a locked filing cabinet, drawer or safe when not in use.

The School operates a CCTV system to protect students, staff and facilities and this is subject to the Data Protection Act and therefore the Data Protection Policy covers the use of images taken by this system. There is a specific Use of CCTV Policy that defines the detailed operational use of the CCTV system in accordance with the Data Protection Act.

Calday Grange Grammar School takes its duties under the Data Protection Act seriously and any unauthorised disclosure may result in disciplinary action.

Subject Consent

Calday Grange Grammar School understands that subjects have certain legal rights to their personal data, which will be respected.

- The school will not process personal data without the consent of the subject, although the processing of data will sometimes be necessary where:
 - The processing is necessary for the performance of a contract to which the subject is party or in the taking of steps with a view to entering a contract.
 - The processing is necessary for compliance with a legal obligation to which the school is subject.
 - The processing is necessary for the administration of justice, legal functions of persons or departments, or functions of a public nature exercised in the public interest.

- Where the processing is necessary for the purposes of legitimate interests of the school, unless the decision prejudices the rights, freedoms or legitimate interests of the subject.

Staff members of the school will be working in close contact with children. Disclosure and Barring Service (DBS) checks will therefore be made a condition of employment.

Sensitive data can only be processed with the explicit consent of the subject, including information relating to a subject's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual orientation, or the commission of any offence.

Sensitive data will only be processed if: It is necessary to protect the subject's vital interests. It is carried out in the course of legitimate activities by a not for profit body or association with appropriate safeguards. It is necessary for the administration of justice or other legal purposes. It has been ordered by the Secretary of State. It is necessary to prevent fraud.

- It is necessary for medical purposes.
- It is necessary for equality reasons.
- It was made public deliberately by the data subject.

Rights to access information

All staff members, parents of registered pupils and other users are entitled to:

- Know what information the school holds and processes about them or their child and why.
- Understand how to gain access to it.
- Understand how to keep it up-to-date.
- Understand what the school is doing to comply with its obligations under the Data Protection Act.

All staff members, parents of registered pupils and other users have the right under the Data Protection Act 1998 to access certain personal data being held about them or their child.

The school aims to comply with requests for access to personal information as quickly as possible, but will ensure that it meets its duty under the Data Protection Act to provide it within 40 working days. The school may make a charge, which they consider to be reasonable on each occasion that access is requested.

However, the school is not obliged to provide unstructured personal data if the administrative cost is deemed to exceed the limit of £450 as contained in the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations.

Publication of information

Caldy Grange Grammar School will publish a publication scheme on its website outlining classes of information that will be made routinely available, including:

- School policies and procedures.
- School prospectus.
- Ofsted Report.
- Minutes of meetings.
- Annual reports.
- Financial information.
- Articles of Association.

Classes of information specified in the publication scheme can be made available quickly and easily on request.

Data retention

The Data Protection Act 1998 states that data should not be kept for longer than is necessary.

In the case of Calday Grange Grammar School, unrequired data will be deleted as soon as practicable.

Some educational records relating to a former pupil or employee of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Copies of DBS certificates will not be taken, although the date that the check was made and the disclosure number will be retained in the school's file and on the Single Central Register.

Keeping Data Secure

The Data Protection Act 1998 requires the protection and security of personal data.

Calday Grange Grammar School will ensure that ICT systems are set up and maintained so that users are assigned access rights appropriate for their role and that these determine the information available to them. Staff will not, as a matter of course, be granted full access to the management information system. Each user will have a unique ID and password. Sharing user ID's is not permitted. Users must not disclose their ID or password details and must not visibly record them on or near to equipment providing access to networks or systems.

Users will change default passwords immediately. Log on passwords should be set with regard to security and should include different characters such as:

- Upper case
- Lower case
- Numbers
- Punctuation
- Symbols

When users are away from their desks a password controlled screen lock must be activated.

Calday Grange Grammar School provides a secure environment for its information. The primary security principle is that information should be kept within this environment and be made available for authorised staff to access. Occasionally it may be necessary to use mobile media to temporarily hold school information.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on equipment owned by the school. Private equipment must not be used for the storage of any personal data.

When personal data is stored on any portable device, USB or other removable media:

- The data must be encrypted and password protected
- The data must be securely deleted from the device in line with school policy once it has been transferred or its use is complete.

All paper based material containing personal or sensitive data must be held in lockable storage cabinets.

On leaving employment with Calday Grange Grammar School staff with access to information sources and systems will immediately have their access rights cancelled.

Secure Transfer of Data and Access out of School

The school recognises that there is a need for data to be accessed by users out of school or for data to be transferred between appropriate parties and agencies. In these circumstances:

- When sensitive or personal data is required by an authorised user from outside school premises, they should, wherever possible have remote access to that information/system.
- If secure remote access is not possible, users must only remove personal or sensitive data from the premises if the storage media, portable or mobile device is encrypted, password protected and transported securely for storage in a secure location. This includes sources of data such as:
 - School laptops
 - External hard drives
 - Paper records
 - School mobile telephones
- Users must ensure that computers or other portable devices which contain personal data are not accessed or used by anybody else when out of school.
- Wherever possible email systems will be avoided in favour of secure transfer systems in relation to sensitive and personal data e.g. School to School, Anycomms, PGP etc.
- If email systems are used to transfer sensitive information then as a minimum the data must be password protected/

Regardless of the method of transfer, the sharing of data which includes personal information will be confined as far as possible, with only essential, relevant information being shared.

Waste Management and Destruction of Data

The disposal of protected data in either paper or electronic form will be conducted in a way that makes reconstruction unfeasible.

Paper based material may be disposed of onsite using shredding machines or through the use of the school's confidential waste disposal service.

To ensure compliance with the Waste Electrical and Electronic Directive and ensure that sensitive data is not accidentally released, disposal of any ICT and associated equipment must be carried out only after reference to the relevant IAO and the in-house destruction of any stored media device such as hard drives.

Challenges and compensation

Calday Grange Grammar School understands that staff members and the parents of registered pupils have the right to prevent the processing of personal data if it is likely to cause damage or distress.

Concerns related to the processing of personal data should be raised with the designated data controller, Calday Grange Grammar School.

Data subjects reserve the right to take their concerns to a court of law and will be entitled to compensation if it is judged that the school contravened the provisions of the Data Protection Act.

Individuals who are not the subject of the data, but suffer damage as a result of the contravention, are also entitled to compensation.

The school will immediately rectify, block, erase or destroy any data that a court of law judges to have contravened the requirements of the Data Protection Act.