Woodlands Academy

DATA PROTECTION POLICY

UPDATED OCTOBER 2018

Contents

INTRODUCTION

Why This Policy Exists

Woodlands Academy (hereafter referred to as 'The Academy') needs to gather and use certain information about individuals.

These can include parents/guardians, students, clients, suppliers, business contacts, employees, volunteers and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled, and stored to meet the organisation's data protection standards — and to comply with the law.

The purpose of this document is to explain what can and cannot be done with this information and **forms an essential part of awareness training for all staff.**

This data protection policy ensures that the Academy:

- Complies with data protection law and follow good practice,
- Protects the rights of staff, clients and partners,
- Is open about how it stores and processes individuals' data, and
- Protects itself from the risks of a data breach.

Safeguarding Against Data Protection and Security Risks

This policy helps to protect the Academy from some very real data security risks, including:

- **Breaches of security and confidentiality.** For instance, information being given out inappropriately.
- **Reputational damage.** For instance, the Academy could suffer if hackers successfully gained access to sensitive data.
- The risk of **large fines** or sanctions being imposed by the authorities.
- The **risks of being sued** for damages by individuals whose data has been mishandled.

DATA PROTECTION LAW AND CORE PRINCIPLES

The Laws

The Data Protection Acts of 1998-2018 (the "Data Protection Acts") and the 2016 General Data Protection Regulation ("GDPR") describe how organisations including our Academy must collect, handle, and store personal information. A new European Union-wide framework known as the General Data Protection Regulation (GDPR) came into force across the EU on 25 May 2018.

An accompanying Directive establishes data protection standards in the area of criminal offences and penalties. This is known as the law enforcement Directive.

The GDPR and the law enforcement Directive provide for significant reforms to current data protection rules. They provide for higher standards of data protection for individuals and impose increased obligations on organisations that process personal data. They also increase the range of possible sanctions for infringements of these rules.

These rules apply regardless of whether data is stored electronically, on paper, or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely, and not disclosed unlawfully.

The Data Protection Acts and the GDPR are underpinned by eight important principles. These, and a description of how they are implemented within the Academy, are described below.

The Principles - Management of Personal Data

All personal data collected and held by the Academy must be managed strictly within the eight guiding principles as set out in the GDPR. **Personal Data must be:**

- **Processed Fairly and Lawfully**

At the time we collect information about individuals, they are made aware of the uses for that information. Where information is disclosed to third parties, this is also set out and explained. This information is set out in the Academy's **Privacy Notices.**

- **Processed Only for Specific Lawful Purposes**

Personal information is only kept for clearly described and explicit purposes. The types of information retained and the specific purposes it is used for and details of any third-party disclosures are set out in the Academy's **Register of Personal Data Records.**

- **Adequate, Relevant, and Not Excessive**

The Academy collects sufficient information to provide an early childhood care and education service to students and their families. The data collected is set out in our Privacy Notices and Register of Personal Data Records.

- **Kept Accurate and Up-to-Date**

The personal data that the Academy collects is checked for accuracy at the time of first collection, and the data subjects (e.g. parents, guardians, staff and others) are given the opportunity to update information freely whenever they are in contact with the Academy over the duration of the period that they attend (students, parents. Guardians) or work in the Academy (staff).

Personal information is retained for such time as required to provide the required services to staff and clients - or to comply with the relevant industry standards, legal requirements or guidelines. These are set out in detail in the Academy's **Personal Data Register with the associated retention guidelines.** Once data has reached the retention threshold, it will be authorised for secure disposal and/or deletion.

- **Processed in Accordance with the Rights of Data Subjects**

Where staff or clients wish to exercise their subject rights in terms of Data Access, correction, or erasure this will be honoured as set out in the Academy's **Subject Access Request handling procedure.**

- **Kept Secure and Protected in Appropriate Ways**

All personal information held within the Academy is kept securely, and protected as described below under Information Security Guidelines, and set out in more detail in the Academy's **Information Security Overview** document.

- **Protected Against Transfer to Countries Without Adequate Safeguards**

No personal data is currently transferred outside the European Economic Area (EEA). If this ceases to be the case, appropriate measures will be taken to ensure the necessary safeguards are put in place and that the target country or territory can guarantee an adequate level of protection

Personal Data and Handling of Special Categories (Sensitive) Personal Data

Personal Data

Under GDPR, '**Personal Data**' means any information relating to an identified or identifiable natural person ('data subject').

In other words, any information that is clearly about a particular person. In certain circumstances, this could include anything from someone's name to their physical appearance.

The definition is wide ranging and in our environment could include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Photographs
- Psychological Reports
- Medical Reports
- School reports
- Staff PPSN numbers
- Birth Certs
- Passports
- Custody documents
- Staff and Parent's Bank Account details
- References
- Health information

and any and all other information relating to individuals. Please note the above is not an exhaustive list.

Special Categories of Personal Data

This is a particular set of sensitive data that can only be collected and used if specific conditions have been met and which must be treated with extra security. The categories are:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data (where processed to uniquely identify someone);
- Data Concerning health

Under GDPR, processing of these special categories of information is prohibited unless certain conditions have been met.

Within the education environment this means that **you must obtain explicit consent from the data-subject** - i.e. the staff member, or parent/guardian(s) - in each case.

You must take care to obtain this consent at the time an employee first joins the Academy or when a parent/guardian or parents/guardians register their Student using the appropriate application or registration forms.

The records of consent should be retained securely for the periods recommended in your **Data Retention Policy.**

RESPONSIBILITIES AND COMPLIANCE

Policy Scope

Everyone who works for or with the Academy has responsibility for ensuring data is collected, stored, and handled appropriately. Each person that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. Specific responsibilities are outlined further in the coming paragraphs.

Woodlands Leadership Team

Persons with responsibility for the implementation of the policy are as follows:

Director	Cecilia Azcunaga
General Manager	Lisa Homan
Academic Manager	Trisha McKinney
Facilities Manager	Denise Coleman
Financial Controller	Alison Hanley
Human Resources Manager	Orla Thomas
Deans Manager	Lucie Favier
Consecrated Team Manager	Janette Serrano

In addition to the above people, Woodlands Academy may engage a contracted Data Protection Officer for periodic visits during the academic year to review progress and ensure implementation of this policy.

- Management will ensure that the basic principles of data protection are explained to staff and parents/guardians. This will be done during staff induction, staff meetings and via emailed communication with Parents.

- There are regular updates to data protection awareness, so that data protection is a “living” process aligned to the way the Academy conducts its business.

- The Leadership Team and / or the Data Controller will periodically check data held regarding accuracy and will complete regular security reviews.

- The Leadership Team will review and update the Data Protection Policy if required, check that any information kept is necessary for running the Academy and along with our IT partners check to see if clerical and computer procedures are adequate to ensure accuracy.

- Non-compliance of the data protection and other policies of the Academy may invoke the disciplinary policy and procedure.

- Confidential and personal information about the Academy's students, parents or guardians and staff will only be shared by Management, Data Controllers, and Designated Child Protection Liaison Persons in relation to child safety, in line with our Child Protection Policy and Safeguarding Statement. Any breach of confidentiality by any member of staff will lead to disciplinary action.

The Data Controller

To ensure the implementation of this policy, the Academy has designated a Data Controller. At present this is Lisa Homan, General Manager. All enquiries relating to the holding of personal data should be referred to the Data Controller in the first instance.

The Data Controller will:

- Inform the person or persons involved a breach of confidentiality has occurred and their personal data may have been compromised. A record of this will be kept on the employee's file or Student's file as relevant.
- Investigate where the breach of security has occurred and invoke the disciplinary policy if necessary.
- Check that additional measures are in place to ensure confidentiality.

- Reassure parents/guardians that the Data Protection Policy has been reviewed and additional measures to ensure security.

- Advise and inform employees and volunteers of the need to ensure confidentiality through additional staff training and re-implementation of the Data Protection Policy.

Employees and volunteers will be required to sign off to confirm they have read and understand the Data Protection Policy and Procedures.

Employee & Volunteer Responsibilities

As an employee, you are responsible for:

- Checking that any information that you provide in connection with your employment is accurate and up to date.
- Notifying the Academy of any changes to information you have provided, for example changes of address.
- Ensuring that you are familiar with and follow the Data Protection Policy.
- Ensuring that any personal data you hold, whether in electronic or paper format, is kept securely.
- Personal information relating to students or their families is not disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party.

Sanctions and Disciplinary Action

Given the serious consequences that may arise, the Academy may invoke the disciplinary policy and procedure in relation to employees. Sanctions include warnings up to and including dismissal for breaching the rules and guideline on data.

In the case of contractors or external service providers, serious breaches of the policies and procedures can and will be deemed grounds for termination of contractual agreements.

Any breach of the data protection policy, either deliberate or through negligence, may lead to disciplinary action being taken and could in some cases result in a criminal prosecution.

Compliance Monitoring and Review

The Academy (with the assistance of the DPO if in place) will undertake regular reviews of the internal operation and changes in the legislation to ensure ongoing compliance with Data Protection Regulation. These will comprise of an annual review.

INFORMATION SECURITY - GENERAL GUIDELINES

Overview

- Access to the information should be restricted to authorised staff on a "need-to-know" basis and where data is needed to carry out their job descriptions.
- Data **should not be shared informally**. When access to confidential information is required, employees and volunteers can request it from the relevant manager.
- The Academy will provide training to all employees and volunteers to help them understand their responsibilities when handling data. This takes place annually on a group basis in September and on a one to one basis for all new employees throughout the year.
- Employees and volunteers should keep all data secure by taking sensible precautions and following the guidelines below.
- Strong **passwords must be used,** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the Academy or externally.
- There should be no legitimate expectation of privacy in terms of content received or sent on work email
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees and volunteers **should request help** from their manager if they are unsure about any aspect of data protection.

Data Storage

The security of personal information relating to students and families is a very important consideration under the Data Protection Acts. Appropriate security measures will be taken by the Academy to protect unauthorised access to this data and to the data it is collecting and storing.

A minimum standard of security will include the following measures:

- Access to the information should be restricted to authorised staff on a “need-to-know” basis. Management will assign responsibilities regarding data at induction. Authorised staff is those identified by management and made known to such staff.
- Manual files will be stored in a lockable filing cabinet located away from public areas.
- Computerised data will be held under password protected files with a limited number of authorised staff.
- Any information which needs to be disposed of will be done so carefully and thoroughly, for example paper documents are shredded and a certificate of destruction kept on file in the main GDPR folder.
- The Academy's premises at Wingfield House have the following security arrangements.
    - Door code
    - Security alarm
    - Locked offices
    - CCTV

  all of which serve to assist in the protection of sensitive data.

If you have any questions or concerns about where or how to store data, please refer to the manager or data controller as outlined above.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.

- Employees should make sure paper and printouts are **not left where unauthorised people could see them** (for example, at the photocopier, left in the bathroom or staffroom or left in unsealed envelopes the cubby holes off reception .
- **Data should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (e.g. a CD or USB key device), these should be kept locked away (and ideally encrypted) when not being used.
- Data should be stored on **designated drives and servers** and should only be uploaded to **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**.
- Data should be **backed up frequently**. Those backups should be tested regularly in line with the Academy's standard backup procedures.
- All servers and computers containing data should be protected by an **approved security software and a firewall**.

Data Use

Personal data is at often at the greatest risk of loss, corruption, or theft when it is being used or accessed:

- When working with personal data, employees should ensure **the screens of their computers/tablets/apps are always locked** when left unattended.
- Personal data **should not be shared informally.**
- Personal data shared by email should be **downloaded, stored securely, and then deleted.**
- Data must be **encrypted before being transferred electronically.**
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

Data Accuracy

The law requires the Academy to take reasonable steps to ensure data is kept accurate and up-to-date.

The more important it is that the personal data is accurate, the greater the effort we will put into ensuring its accuracy. It is the responsibility of all employees and volunteers who work with data to take all reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated** (for instance, by updating parent's contact information).
- The Academy will make it **easy for data subjects to update the information** held about them, over the phone, or by email or on TMS.
- Data should be **updated as and when inaccuracies are discovered**. For instance, if a member can no longer be reached on their stored telephone number, it should be removed from the database.

Data Disclosure to Third Parties

The Academy is ultimately responsible for any personal data passed to third parties and care must always be given to procedures and security.

The only data disclosed to third parties in the normal course of events is as described in the Academy's Privacy Notices and Register of Personal Data Records.

In certain circumstances, the Data Protection Acts allow personal data to be disclosed to external agencies without the consent of the data subject. Any requests from external bodies and agencies not specifically provided for in legislation including An Garda Síochána, should be in writing.

Under these circumstances the Academy will disclose requested data; however, the Data Controller must ensure the request is legitimate, seeking assistance from Management and from the Academy's legal advisers where necessary.

Please note that information may need to be disclosed to authorised third parties. The Academy will always check validity of any requests made.

The following list includes examples of such organisations but is not exhaustive:

- An Garda Síochána
- The National Board for Safeguarding Children in the Catholic Church in Ireland (NBSCCCI)
- TUSLA
- ACELS
- Our contracted Health & Safety Manager
- Insurance Company
- Health and Safety Authority
- Workplace Relations Commission
- Revenue Commissioners
- Health Insurers
- Travel Agencies
- Oak promotion teams
- Events coordinators
- Retreat Centres
- Sodexo
- Sporting groups, local Irish schools for sporting events
- Activity Centres
- Other Professional Advisors
- Achieve
- Wriggle
- Advance Systems Ireland
- Cambridge
- TIE
- Medmark
- Emilina Ellis Child Psychologist
- Hair Force
- Dr. Leah Roche GP

- School Photographer
- Health Practitioners (optician, Orthodontist, podiatrist etc)

Please note that where information may need to be disclosed to authorised third parties, **it is essential to always check validity of any requests** made before release of the data.

Note: Data Collected Through Garda Vetting
The Academy understands that sensitive information may be identified through Garda Vetting. In the event that an employee's Garda vetting raises concerns the information will be dealt with on a confidential basis. All information pertaining to such a situation must be stored in the same way as other data. The Academy will not pass on a copy of an employee's Garda Vetting Form to any other party. The Academy will hold original Garda Vetting forms.

We will also hold copies of police checks for staff who have lived in other countries (from age 18 years). The staff member holds the original and we hold a certified copy.

Data Erasure and Disposal
When documentation or computer files containing personal data is no longer required, the information must be disposed of carefully to continue to ensure the confidentiality of the data.

For paper-based files and information no longer required, employees and volunteers should safely dispose of documents or media in shredders. Shredding machines are available in the following areas:

1.
2.
3.

In the case of personal information held electronically, temporary files containing personal information should be reviewed regularly and deleted when no longer required.

When personal data reaches the point where the retention period has expired, the information should also be securely deleted and removed.

In the event that IT equipment containing personal data is no longer required, all data stored on the devices must be removed prior to disposal.

CCTV

Woodlands Academy is responsible for the data/information collected using CCTV.

Usage of CCTV is in line with the principles set out in **The Data Protection Acts of 1988 and 2003,** and the **2016 General Data Protection Regulation (GDPR):** Where CCTV contains footage of images which can be clearly identified as a recognisable person, it is deemed to be Personal Data and is covered by the Data Protection Acts and Regulation. In short, where a data controller uses a CCTV it is obliged to comply with all associated data protection obligations.

Purpose of the CCTV

The system has been installed by the Academy with the primary purpose of ensuring the safety of students in our care, and helping to ensure the safety of all staff, parents/guardians and visitors, consistent with respect for the individuals' privacy.

This will be achieved by monitoring the system to:

- Ensure that students are safe,
- Assist in the prevention and detection of crime,
- Facilitate the identification of any activities/event which might warrant the invoking of the disciplinary process for students (eg pranks)

- Facilitate the identification of any activities/event which might warrant the invoking of the disciplinary policy and procedure for staff
- Provide opportunities for staff training, and
- Investigate accidents.

The system will **not** be used:

- To provide recorded images for the Internet,
- To provide images for a third party other than An Garda Síochána, NBSCCCI or TUSLA, during their enquiries,
- For continuous monitoring of staff,
- For monitoring staff performance,
- As a supervision tool, or
- For recording conversations.

Note: If after viewing the CCTV for any of the reasons stated above, incidents of inappropriate practice or breach of policies are observed, these can be brought to the attention of the employee. The employees / volunteers should be given the opportunity to view the footage. Depending on the circumstances, this may result in the discipline policy and procedure being invoked.

Fairness

The Academy and its management respect and support the individual's entitlement to go about his/her lawful business, and this is the primary consideration in the operation of CCTV.

Although there will be inevitably some loss of privacy with CCTV, cameras are not used to monitor the progress or activities in the ordinary course of lawful business. They are used to address concerns, deal with complaints, or support investigations. New employees and volunteers will be informed immediately at induction that a surveillance system is in operation. Parents/guardians will be informed when they enrol their daughter. They will be informed of the purpose of the CCTV and what it can and cannot be used to monitor.

Responsibilities of Management

Management is responsible for the operation of the system and for ensuring compliance with this policy. In particular:

- To ensure the system is always operational,
- To ensure that servicing and repairs are carried out as necessary to the system,
- To respond to any individual's written request to view a recording that exists of him/her or his/her daughter,
- To ensure prominent signage is in place that will make individuals aware that they are entering a CCTV area.
- To ensure that areas of privacy (toilets etc.) are not monitored using CCTV, and
- To ensure confidentiality is maintained at all time.

Recorded information is held on the server and will only be available to those directly connected with achieving the objectives of the system.

Location of Cameras

The choice of sites for locations of CCTV Cameras will be in line with the primary purposes outlined above, i.e. where they assist in ensuring the safety of students and the safety of all staff, parents/guardians and visitors. Cameras will not be in areas where people expect to have a reasonable expectation of privacy.

- The following areas are currently monitored by CCTV:
- Main gate to Woodlands
- Car park area outside the front door
- The front door
- Kitchen door at the back of the building
- Door at end of school corridor out to car park at the back
- Bedrooms in school area
- Lockers
- Laundry
- Corridor outside downstairs offices

Signage

Signage is displayed advising that CCTV is in operation for ensuring the safety of students in our care, and helping to ensure the safety of all staff, parents/guardians and visitors.

Right to View or Access Recordings

In line with the requirements of the GDPR, data subjects have the right to request access to their images or personal data captured by CCTV. The Data Controller will respond to a request to view a recording by allowing the viewing to take place in the presence of management on the premises. This is to protect other students/staff that may be present on the recording.

Sharing or Copying Recordings with Data Subjects (i.e. parents, guardians, or staff)

Any person whose image is recorded on a CCTV system also has a right to seek and be supplied with a copy of their own personal data from the footage. To exercise that right, a person must make an application in writing or by email. The data controller may not charge for responding to such a request and must respond within 30 days.

In the first instance, the individual should be asked whether they would be satisfied with merely viewing the images recorded.

Recordings will however be provided, where formally requested by parents, guardians, or staff.

- Requests for access to recordings must be made in writing, or by email.
- Sufficient information must be provided to locate the relevant recording, a specific date, and reasonable time window.
- Viewings will take place, if appropriate, in the Academy in the presence of management.

- The DPO will have 30 days to respond.
- If a copy of recording is given to a third party, that third party must sign a declaration form that they will not share the tape with anyone else, copy it, or use it for unauthorised purposes.
- An incident report will be completed for each incident requiring investigation.

If access to or disclosure of the images is allowed, then the following should be documented:

- The date and time at which access was allowed or the date on which disclosure was made,
- The identification of any third party who was allowed access or to whom disclosure was made,
- The reason for allowing access or disclosure,
- The extent of the information to which access was allowed or which was disclosed, and
- The identity of the person authorising such access.

Where images of parties other than the requesting data subject appear on the CCTV footage, the onus lies on the Academy to pixelate or otherwise redact or darken out the images of those other parties before supplying a copy of the footage or stills from the footage to the requestor.

If the system does not have the facilities to carry out that type of editing, an editing company may need to be hired to carry it out. If an editing company is hired, then the Manager or designated member of staff needs to ensure that there is a contractual relationship between the Data Controller and the editing company.

Sharing of CCTV Images with Garda Siochana or other Authorised Third Parties

At times it may be necessary at times to provide copies of recordings to An Garda Siochana or other authorised parties.

CCTV footage should only be provided to An Garda Siochana when a formal written request is provided to the data controller stating that Garda Siochana is investigating a criminal matter.

For practical purposes, and to expedite a request speedily in urgent situations, a verbal request may be sufficient to allow for the release of the footage sought. **Any such verbal request must be followed up with a formal written request.** It is recommended that a log of all Garda Síochána requests is maintained by data controllers and processors.

There is a distinction between a request by Garda Síochána to view CCTV footage and to download copies of CCTV footage. In general, Garda Síochána making a request to simply view footage on the premises of a data controller or processor would not raise any specific concerns from a data protection perspective.

For authorised third parties, similar rules apply - copies of CCTV footage can be viewed or made available subject to the requirements and restrictions as set out above.

Storage and Retention of CCTV Footage

The storage medium is stored in a secure environment and a log of access is kept. Access is restricted to authorised personnel:

1 Cecilia Azcunanga
2 Denise Coleman
3 Racine Silva
4 Lucie Favier
5 Lisa Homan

Traceability

Recordings must be logged and traceable throughout their life in the system. They must be identified by a unique serial number indelibly marked on the media shell.

Time and Date Stamping

The correct time and date must be overlaid on the recording image.

Retention Period

Recordings will be retained for no longer than 30 days (or as defined in the Academy Personal Data Register & Data Retention policy) - unless there is requirement to retain CCTV footage to assist with the investigation of incidents, accidents, or other serious issues.

DATA BREACHES

Definition: A data breach is an incident in which the Academy's employees', volunteers or students' **personal data has been lost, accessed, and/or disclosed in an unauthorised fashion.**

This would include, for instance, loss or theft of a laptop containing student or staff details, an email with personal information being sent to the wrong recipient, as well as more organised incidents of external hacking.

Your Responsibility and Immediate Action Required

All employees and volunteers have a responsibility to take immediate action if there is a data breach.

- If an employee suspects at any time and for any reason that a breach may have occurred, then there is a **need to report it to the General Manager as an urgent priority.**
- Once notification of an actual or suspected breach has been received, the General Manager will put the **Data Breach Procedure** into operation with immediate effect.

DATA SUBJECT RIGHTS/SUBJECT ACCESS REQUEST HANDLING

Privacy Notices

The Academy aims to ensure that individuals are aware that their data is being processed and that they understand:

- How the data is being used, and
- How to exercise their rights.

For parents of students this is set out in the Academy's **Privacy Notice**, provided when they first apply to enrol their daughter with Woodlands. A version of this statement is also available on the organisation's website.

For new staff members, this is set out as part of the contract and induction material supplied at time of recruitment.

Subject Access Requests

All individuals who are the subject of personal data held by the Academy are entitled to:

- Ask **what information** the Academy holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the Academy is **meeting its data protection obligations**.

If a person the Academy requesting this information, this is called a Subject Access Request.

The handling of access requests is described in more detail in the **Subject Access Request ("SAR") Handling Procedure.**

***