The Angmering School

GDPR
Policy 2020

General Data Protection Regulation Policy Document

Reviewed MGI
Approved at Governing Body meeting 9th December 2020
Next review due 2022

Contents

Revision History

Revision	Date	Author / Editor	Comments
1	16/05/18	Marc Ginnaw	
2	26/11/2020	Marc Ginnaw	

Terms

2FA – Two Factor Authentication
AES – Advanced Encryption Standard
API – Advanced Programming Interface
AUP – Acceptable Usage Policy
BIOS – Basic Input/Output System
WSCC – West Sussex County Council
DPIA – Data Protection Impact Assessment
DPO – Data Protection Officer
GDPR – General Data Protection Regulation
ICO – Information Commissioner's Office
MIS – Management Information System
PII – Personnel Identifiable Information
PP – Pupil Premium
SEN – Special Education Needs
Phish – To fraudulently obtain security credentials by means of a fake login screen
TLS – Transport-Level Security

Introduction

The Angmering School ("us", "the school", "the organisation" or "we"), ICO registration Z6933184**,** is a secondary school located in the United Kingdom. We act as the controller for all data relating to employees and students.

The Angmering School has reviewed its processes, its data sub-processors, and is providing guidance, along with this document, to staff to ensure full compliance with GDPR.

The flow of all personal data has been logged and all personal data processed has been recorded and is frequently reviewed.

This document details the requirement to which The Angmering School need to abide to be GDPR compliant.

We are committed to protecting personal data, ensuring it is processed and recorded fairly, and stored safely. We promote a data protection mind-set where the protection of data is always considered alongside the requirement of the school.

Everyone in the organisation is obliged to take responsibility for data protection and this isn't just to comply with legislation, it is to ensure both staff, students, and parents are comfortable with our data processing activities. Data breach fines are now up to €20,000,000 and, although fines levied will be on a case-by-case basis meaning a fine for the school would be smaller, a fine would damage our reputation and financial stability.

Scope of the Policy

This policy applies to all school employees carrying out activities on behalf of the school.

For the purposes of this policy, any individual not acting for an organisation, whether paid or not, such as, but not limited to, a governor or parent helper, is an employee.

This policy applies to any personal data that the school processes or stores including, but not limited to, current, future and ex staff and students and their personal contacts such as parents and next of kin.

Data Management

The Data Protection Officer role has been assigned to the IT Services Manager Marc Ginnaw.

Decision makers and key people in the school agree to support data protection legislation and promote a positive culture of data protection compliance across the organisation. 'Data protection by design' is encouraged during and beyond all new data processing activities.

The flow of all personal data has been logged and all personal data processed has been recorded and reviewed.

Training

The Angmering School guides all employees in the General Data Protection Regulation and provides updates as and when required; this document is part of employee GDPR training and all staff are expected to read it. Further guidance can be found on the staff website under 'ICT Acceptable Use' and 'GDPR General Data Protection Regulation Guidance for Staff', which all staff are expected to read. Employees are also encouraged to discuss with senior staff any training needs, concerns or risks, and to make contributions to the organisation's data protection policies or procedures.

Managing Information Risk

We are the data controller for employee and student data and ensure its security according to this policy. A Data Protection Impact Assessment is carried out for all identified data risks.

Data We Control

Please see our privacy notices on the school website

Individual Rights and Rights of Access

We store information on employees and students throughout their employment or education and for a period beyond.

Right of access requests are to be made by emailing gdpr@theangmeringschool.co.uk

Right to Rectification and Data Quality

Past and present employees and students have the right for data to be rectified if found to be incorrect.

Please forward any requests to gdpr@theangmeringschool.co.uk

Right to Erasure Including Retention and Disposal

Personal data will not be retained by the school for longer than necessary in relation to the purposes for which they were collected

To request data to be disposed of please email gdpr@theangmeringschool.co.uk

The school has a legal requirement to store some data and will advise if it cannot be destroyed for this reason.

Right to Restrict Processing

All data subjects have the right to restrict data processing and all requests are to be emailed to gdpr@theangmeringschool.co.uk

The school has a legal requirement to process some data and will advise if processing cannot be restricted for this reason.

Right of Data Portability

For any students leaving the school, all relevant data is transferred to the new school. Student files can be transferred by request by contacting itsupport@theangmeringschool.co.uk

Data Security and Encryption

The Angmering School processes personal data in a manner that ensures appropriate security.

Data Sub-processors

The Angmering School uses data sub-processors and has assessed them for data protection compliance.

Data Protection by Design

Staff must balance data protection with the school need and usability; do not compromise security for usability. The ICO suggest measures such as data minimisation, pseudonymisation and transparency measures. A working example of pseudonymisation would be to use initials instead of a name for a care-pack being taken on a trip. The school

must also consider the safety of student so it is essential to ensure that there was no confusion over identity.

Lawful Processing

We keep a record what individual data is processed, and ensure that there is a legal basis for doing so.

Data Protection Guidance for Staff

What is Personal Data

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified including by referencing a code.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data and paper student reports.

Personal data that has been pseudonymised, e.g. key-coded, can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Special Category Personal Data

Special category data is more sensitive, and so needs more protection. For example, information about an individual's:

- Race
- ethnic origin
- politics
- religion
- trade union membership
- genetics

- biometrics (where used for ID purposes)
- health
- sex life
- sexual orientation

In particular, this type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

What is a Personal Data Breach?

It is not simply someone getting hold of personal data; it is also the destruction or altering of personal data such as a child getting into SIMS and setting negative behaviour to positive. The school losing all SIMS data and having no backup would be regarded as a huge breach. In this case the school would normally report to the ICO and it could result in a fine, but a child changing their records would normally be dealt with internally with no further action.

This is the ICO's definition of a personal data breach:

'A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.'

Data Breach Notification

In the event of a data breach, including but not limited to, lost equipment or hacked email account, employees must, as soon as practical and without any unnecessary delay, notify the DPO, or in their absence, a member of the headship. Never cover up a data breach, however small, as doing so is likely to make matter worse. Many data breaches notified to the ICO are recorded without fines being made, but any breaches where dishonesty is involved would most likely result in a fine. Data controllers have a duty to notify the ICO of a breach within 72 hours of becoming aware of it, where feasible, if the breach is likely to risk people's rights and freedoms. If it is not likely to risk people's rights and freedoms, they must be able to justify the decision and therefore need to document it.

All data breaches must be logged internally by contacting the DPO.

It has been mentioned that employees must notify internally as soon as practical but the first task is to contain the breach to minimise impact. This could, for example, be in the event of your Google account having been phished. The priority here would be to stop any further access to your account. As every breach is different, you need to use your professional skill and judgement to decide on how to carry this out, but will always entail contacting the DPO.

In the event that you find a system or process which you suspect is not compliant with this policy or the objective of information security you have a duty to inform the DPO so that they can take appropriate action.

What are the Lawful Bases for Processing Data?

Most lawful bases require that processing is 'necessary'. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks).

Printing Personal Data

Staff are instructed only to print personal data if necessary and, if it is printed, to ensure it is shredded before disposal. A cross-shredder is located in the main admin office, the staffroom, and the reprographics room for staff use.

Clear Desk Policy

All printed personal data should be either in the possession of an employee, in a secure office during the day, and locked away at night. Staff are encouraged to be as tidy as possible to reduce the risk of lost data.

Conversations

Staff should be aware of their surroundings when having a conversation about a data subject. It is unacceptable to discuss anything about an employee or student when there are students or members of the public present. An example of a data breach is saying in front of a student 'Employee A was late today' or, in an office area, with members of the public present 'student A has been late again'. Although you may only state a first name, this may be sufficient for a person to be identified using the context of the conversation.

Signing in and out

To protect your own privacy do not write personal reasons for leaving site in the signing out book, instead writing 'personal'. In all instances of leaving the site, you must first have the agreement from your line manager.

Radio Communication

Two-way radio communication is encrypted so that only school radios can hear the conversations, but transmissions can be overheard internally by nearby students and visitors. With this in mind, it is essential to anonymise all conversations ensuring you never refer to a student by name, except in a situation where such communication is necessary to protect a person.

Password Requirements Policy

Each employee password must be:

- Unique across all other accounts and systems
- 8 characters or more

- Contain a mixture of alphanumeric and special characters, including both upper and lower-case letters
- Never written down on paper
- Not shared with any person except where necessary to complete your tasks. In this case agreement with the DPO is necessary

Note: 2FA (two factor authentication) must be used for all staff Google accounts.

If you lose access to one of your accounts, you must contact IT support in order for them to verify your identity and reset your password.

Identity Verification

At times you may be asked to amend a student record or change a password to gain access to an account. In circumstances such as these, and any similar ones, ensure you verify the identity of the requester and ensure that they have authorisation to request such actions. An example of confirming identify would be to ask a parent for the student middle name and date of birth.

Google Drive

Google Drive poses a data risk if not used correctly and users must always take care when sharing. Drive should always be used in place of emailing attachments as it possible to unshare a document whereas it is not possible to retrieve mistakenly sent emails. To ensure data is protected, please follow the guidance below when sharing Google Drive documents:

Link Sharing

On – Public on the web. This is only to be used for files hosted publically on a website.

On – Anyone with the link. This should only be used when sending public information out by email. This setting must never be used for internal communications, instead users should send to the relevant groups or, if for whole school internal communication including students, you can use the two methods below.

On – The Angmering School. To be used for whole school communications not containing personal data such as newsletters.

On – Anyone at the Angmering School with the link. To be used for whole school communications not containing personal data such as newsletters.

For the above, the files must not contain personal data unless agreed by the individual using official Angmering School consent.

Off – Specific People. This allows you to choose exactly who has access and must be used when sharing confidential data.

Email

Staff must not send personal data unencrypted for students to new schools and must use secure methods as advised by WSCC.

All data in emails is subject to being requested by the data subject, such as an ex-student requesting all correspondence on them. Please bear this in mind when communicating and only ever write something you would be happy for the data subject, or their parent, to see.

You are required not to reference the subject of personal data publicly, or via systems or communication channels not controlled by the school, for example, the use of external e-mail systems not hosted by the school, encrypted or otherwise, to distribute anything that may contain personal data is not allowed.

Staff should actively avoid sending student or staff data in email as it is difficult to control the retention of data stored this way. Where possible, anonymise using initials or another suitable method. All whole school communications with information about students should be sent to the forum group account for that year. The group will be deleted a period after the academic year as the data will no longer be relevant.

Staff must ensure that the recipient is correct, especially when sending to staff, as some students have the same name as staff. Please follow the guidance below on email accounts construction:

Staff initial and last name – ilastname@theangmeringschool.co.uk

First four letters of the last name, initial and a 2 digit number –lasti17@theangmeringsch...

Any messages sent to students containing personal data is a data breach and the DPO to be notified if this occurs.

Visitors

Visitors to the school must be escorted by an authorised employee at all times. If you are responsible for escorting visitors, you must restrict them appropriate to areas.

Staff Identity Badges

These badges give access to your print queue and the school gates, therefore potentially giving access to confidential data and allowing students to go off site. For this reason, badges should always be kept secure; do not allow students to use your badge to access the copiers or for any other reason.

Staff Leavers

Staff leaving employment from the school will be required to return all records, in any format, containing personal information. Any remembered personal data must be forever kept confidential.

Portable Storage Devices

Any information being stored on a portable device, such as a USB stick or laptop, must be encrypted and logged by the IT department to ensure suitability. If there is any doubt regarding the requirements, seek guidance from the DPO.

All portable storage devices used are to be recorded by IT support and from time-to-time you will be asked to confirm that you still have the device, but it is still your responsibility to report any losses as soon as they occur.

Data Transfer

Data that must be moved within the school is to be transferred only via business provided secure transfer mechanisms such as school Gmail, Google Drive, or the staff shared drive; you must not use other mechanisms to handle personal data. If you have a query regarding use of a transfer mechanism, or it does not meet your business purpose you must raise this with the DPO before attempting to use it.

Transfer of electronic Exam Papers and Coursework

Any exam related work being transferred to exam boards must be sent securely by either data transfer or, if required, disks and portable storage must be encrypted and the password transferred separately.

General Computer and Data Security

You must always lock your computer when away from it and never let a student use your account. The exception to this rule is for a student to use the classroom projector to present to the class, however, this must be supervised by you.

Please ensure that assets holding data within the scope of this document are not left unduly exposed, for example visible in the back seat of a car.

Staff Personal Devices and Working from Home

The school encourages staff to use personal devices to access work resources to enable flexible working, however, you must be certain that data you are accessing is secure.

If you work remotely you must take extra precaution to ensure that data is appropriately handled. Shared accounts and public computers should never be used to access any school systems.

Personal computers can be used to access the VPN or other online resource but no personal data is to be downloaded to the computer or printed off-site. When using a personal computer you must always use an account that no other person has access to in case of your password being saved by the internet browser thus giving access to your account.

iPad and iPhone

Encryption is automatically enabled as soon as you set a passcode on your device so it is therefore it is essential you do this before accessing any school resources on it. This code must be secret to you and no other people should use the device without your supervision.

Android Devices

Android devices from version 6 (Marshmallow) onwards are encrypted as soon as you set a passcode on your device so it is therefore it is essential you do this before accessing any school resources on it. This code must be secret to you and no other people should use the device without your supervision. If you have an android device prior to version 6 please speak to IT support prior to accessing school resources on it.

Chromebook

The Google Chromebook is encrypted and can be used to access your school account.

Recording of Telephone Conversations

External telephone calls can be recorded for training and safeguarding purposes using the Mitel client. The recordings are saved to your voicemail and must be treated securely in the same way as any other personal data. Do not record calls with other members of staff as this is an inappropriate use of the system.