UK General Data Protection Guidance for Acorn Education Trust Staff

Acorn
Education Trust

Acorn
Education Trust

UK General Data Protection Guidance
for Acorn EducationTrust Staff

Contents Page

All members of Acorn Education Trust are expected to comply with UK General Data Protection Regulations (GDPR)

We have a right to collect and retain certain information about the students in our care, our workforce and the people who visit our settings. But we only have the right to hold on to it for as long as we need it - and while we hold on to it, we have a duty to take care of it.

If you have any queries or concerns about data protection in school, please contact the following (in order):

- School GDPR leader
- Acorn Education Trust GDPR Leads (Jo Ronxin or Fiona Richards)
- Data Protection Officer
  Judicium Consulting Ltd
  dataservices@judicium.com
  0345 5487000

The Information Commissioner's Office (ICO) is the regulator for data protection. If there is any breach of data protection laws, the ICO will be the ones to handle the matter, issue guidance and in extreme matters, issue fines.

Six Basic Principles
# of GDPR for staff to remember

1 Keep personal data private and secure

2 Delete personal data you don’t need to keep

3 Know what you are using the data for and how long you will keep it

4 Ensure you have the relevant permissions before sharing personal data (for example posting photos on social media)

5 Should you receive data requests pass them on to your line manager/DPO straight away

6 Don’t take personal data home or transfer data onto personal devices without permission or suitable security in place

Policies and Privacy Notices

Policies

All schools within Acorn Education Trust are expected to adhere to the GDPR policies. All Trust GDPR policies can be found on the Acorn Education Trust website: **www.acorneducationtrust.com**

Privacy Notices

What is a privacy notice?

This is a notice which details to individuals the personal data we use, why we use it and their rights over their data. How do we communicate a privacy notice to parents? Parents should be given a copy of this notice by email, or in hard copy when their child joins the school and the notice should be readily accessible (e.g. on the website, in the reception area). Schools should also consider including the privacy notice in the new school year information pack for pupils/parents.

What is the difference between a privacy notice and a data protection policy?

A privacy notice is a document to give to individuals communicating how you use their data and their rights.

A data protection policy is an internal document which sets out the processes and procedures your school has adopted in order to ensure compliance with data protection laws in the processing of personal data.

Does a privacy notice have to be signed by parents?

No, a privacy notice does not need to be signed by parents.

Data Breaches

A data breach is a compromise of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to protected data - essentially anything that affects its confidentiality, integrity or availability.

e.g., forwarding an email to the incorrect recipient containing personal information.

I feel that a breach has occurred. What do I do?

- Don’t worry!
- Act quickly (72-hour turnaround)
- Report it immediately to your Headteacher/GDPR manager
- Try to contain the breach- e.g. recall email
- Are there any additional factors/circumstances which should be known?
- Don’t dawdle and don’t ignore!

How to Avoid Data Breaches

- Use approved communication systems
- Check and re-check recipients of emails
- Take care to upload the correct attachments
- Be aware of the content of email threads when forwarding to others
- Blind copy to hide the email addresses of others

Data Requests

A Subject Access Request (SAR) is simply a request made by or on behalf of an individual for the information which they are entitled to ask for under section 7 of the Data Protection Act 1998 (DPA).

We have to respond without undue delay and within one calendar month. We can only provide information if we have it - therefore:

a) Delete emails regularly

b) Never discuss a named subject in private communication systems as this is disclosable to subjects

What information can parents see about their children?

Anyone can make a request to see the data that the school holds about them. This may include a parent making a request on behalf of their child.

As for the data that they can have - it is any recorded data that is held about them. This includes emails and paper documents. Each request has to be treated individually. For example, if there are safeguarding or legal issues surrounding the child and/or parents, we might need to carefully consider if we can release this data.

What is Freedom of Information and how does it relate to data protection?

Freedom of Information does not necessarily concern personal data. Schools are no different from other public bodies and have to answer these requests for information.

It is aimed at providing the public with transparency about how public bodies are run, making these bodies more accountable to the general public. Common examples of documents disclosed as part of Freedom of Information include minutes from governor meetings, policies as well as general financial data.

What is the difference between a Freedom of Information Request and Subject Access Request?

Individuals often get the two confused.

But in short, a subject access request usually involves asking for personal information about someone. Freedom of information requests usually ask for non-personal data and are commonly made by journalists who may be seeking a story or companies who are wanting to sell the school a product. Some requests can incorporate elements of both.

For example, a parent asks why their child has not been granted SEN support. The general policies and procedures that lead up to the decision would normally be released under a FOI request. Individual data about the case itself and decision would be released under a subject access request. In both instances, these requests need to be responded to within a set timeframe so if you do receive one do forward it to your GDPR lead in school.

Data Protection
and Social Media

All staff should be careful about giving out personal details over social media. Staff should assume their accounts are visible to others and therefore check their own privacy settings and should not befriend students or parents.

Personal social media accounts (e.g., WhatsApp, Facebook Messenger, personal email accounts…) should not be used for work related business. Please be aware that personal accounts, if used for work, are open to Subject Access Requests.

If and when you are in charge of school accounts, please consider the security settings and who can access them. Students and parents should also not be befriended from school accounts.

All staff need to adhere to the Acorn Education Trust code of conduct while on social media.

Data Protection and Consent

In certain situations, we may need to obtain consent.

The most common example of this is using student photos. Schools must gain positive consent and cannot assume that it is given; it should be specific.
Photos of students must not be taken on personal mobile devices.

What is the age a child can give consent in the context of the GDPR?

There is no legal age but the requirement is that we should seek consent from the child if they are old enough to understand what they are consenting to, otherwise the consent is not 'informed' and therefore is invalid. Whilst there is no set age, there is an assumption that a child aged 12 and over would be deemed old enough to understand their data rights. This is again dependant case to case (for example if the child has particular learning difficulties).

If a child cannot give consent then who can?

This will normally be a parent who can consent on the child's behalf if they are too young.

Do I have to gain consent for everything I share?

No - the rule is that you must gain consent where there is no other lawful basis to use the data. The main lawful bases are consent, to comply with a contract, legal obligation, vital interests, public task and legitimate interests.

Am I allowed to write full names on leavers' hoodies?

Schools need parents or the student to opt in (give their consent) to having the child's forename and surname on the back of the hoodie. This permission can be when they are confirming their agreement to purchase a hoodie but just make sure they are aware that full names will be on the hoodie at the time of purchase.

Can I take photos and videos of pupils?

Yes, but permission is needed from parents/guardians (or from the student if they are old enough to consent), to both take and use images and videos for publication or general display. Where pupil photographs are used for identification purposes, e.g. on their pupil record, permission is not required as the school can rely upon using public task as the legal basis for processing.

Do I need to delete pupils' photographs from the school website at the end of each year?

You do not need to delete photographs from the school website each year. However, the school should be clear about the length of time the image will be kept. This will usually be throughout the child's life at the school. You will only need to delete these photos from the website once the time period for retention has lapsed.

Can I allow parents to take photos at sporting and drama events?

This is up to the school to determine. There is no requirement that schools adopt a "no photography" rule for sports, music or drama events. GDPR does not apply to parents taking pictures for their own personal use. Your school may have clear guidance regarding parents taking photographs, for example there may be a rule that parents may not post photos or videos of school events on social media sites except for their own children. The key is to work with the parents and agree a way forward before the event. Where a school event includes children, who have previously refused consent for photos, your school must decide how to manage this.

Do I need permission from parents/guardians to display a child’s photo with medical needs within school?

As stated above, a school may use photographs without gaining consent in certain situations. In this instance, they are used in order to identify children at risk of requiring urgent medical intervention which forms part of the school’s duty of care and public task. If you are not seeking permission you should still inform affected parents/guardians that this is being done. You should ensure that these details are hidden from third parties e.g. in the staff room, behind a curtain or a locked room - to prevent casual access.

Data Protection Impact Assessments

Schools must conduct a data protection impact assessment (risk assessment) when introducing new software or technologies which affect personal data. You must be aware of how third parties will use the personal data you provide them with (processors).

Purpose and Benefits of a DPIA

- To consider issues prior to implementation
- To consider risk
- Accountability

What to Include In a DPIA?

Your DPIA must:

- Describe the nature, scope, context and purposes of the processing
- Assess necessity, proportionality and compliance measures
- Identify and assess risks to individuals
- Identify any additional measures to mitigate those risks
- Acorn Education Trust keeps a central record of all DPIAs in place - can be adapted for your own setting

GDPR and Technology

What is encryption and why is it important?

Encryption is the process of protecting data from people who you don't want seeing it. For example, using a secure web page when inserting credit card details. With emails it is normal practice for them to have some level of encryption (Microsoft and Google state that they have encryption). Most 'cloud' storage is also transferred through encrypted connections. You can also encrypt devices such as laptops.

The Information Commissioner's Office (ICO) recommend that organisations should use encryption where possible. This will depend on the data being used and the risk to the organisation.

For example, if you use laptops which are kept on site and locked away then there is less need to encrypt the laptop. However, if those laptops are taken home and they may contain sensitive data on those devices then it would be recommended to encrypt the laptop.

Can I use my own personal computer/tablet to look at pupil's personal data or school email?

It is not advisable. There are dangers in using your own device for accessing pupil data or your school emails. These dangers are mainly around other people seeing the data, whether this is accidental or not, with many computers and tablets at home. There are also issues with the settings that you might have set on your tablet or computer. It is common for devices to automatically backup data in cloud storage. So holding photos taken on a field trip could mean that pictures of students could be stored on your personal cloud storage.

Can I use my personal USB memory stick to take files home from school?

If the files contain zero personal information (such as planning), yes, although there are much better options, such as using the school network to transfer data. For files containing personal data, you should not use your own.

Data Protection when you leave employment with Acorn Education Trust

If you leave employment with Acorn Education Trust you need to ensure that all personal data you hold on subjects is returned, disabled and/ or deleted. This includes any personal devices, including USBs and laptops.

Example Case

Headteacher in Twickenham was fined by a court for using personal data on students from his previous schools, which he had uploaded from his own USB stick onto his new employer's servers.

School´s Data Protection

- Pass on data requests without delay to your DPO
- Report any data breaches to your DPO immediately
- Lock away paper records
- Don’t write your password down or store your password in your web browser
- x2 Duplicating personal data is unnecessary
- When discarding personal data shred it or put into confidential waste bins
- Verify the individual before handing over data
- Don’t leave personal information lying around
- Don’t download data onto a personal device unless authorised
- Remember to log off

If in doubt contact your DPO

School´s Data Protection

- Lock your computer when away from your desk
- Don’t give out passwords or security info
- Send sensitive communication securely
- Clear your desk at the end of the day - remove sensitive data
- Check before using your own USB or hard drive
- Password protect devices used to remotely access emails
- Report any potential security breaches, malware, or phishing emailis to your PDO
- Think twice before sending emails, to avoid sending to the wrong person
- Don’t leave photocopying lying around
- If you are unsure, better to ask your DPO

If in doubt contact your DPO