General Data Protection Regulations Compliance Guidance

Contents

(If you are viewing this document online, click on the headings below to jump to the relevant section)

1. Introduction

This guidance document provides an overview of the General Data Protection Regulations (GDPR) and details suggested actions that schools and academies may wish to consider now. Please note this guidance document will be reviewed and changed regularly as we receive further information on the planned new regulations

The General Data Protection Regulation (GDPR) will replace the existing Data Protection Act 1998 and remain as the governing law for data protection matters until the enactment of the new Data Protection Act (expected in the first half of 2018), which will incorporate the GDPR into the legal systems of the UK regardless EU membership status.

Although the fundamental principles of data protection are remaining broadly the same as under the previous Data Protection Act, an important alteration is the addition of the new accountability principle.

This new accountability principle demands that every school processing personal data implements appropriate technical and organisational measures that ensure compliance can be demonstrated at all times.

What is personal data for the purposes of GDPR?

The GDPR widens the scope of what is considered Personal Data to a purposefully broad definition: “any information relating to an identified or identifiable natural person.”

What is “Processing”?

The GDPR defines processing as “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.”

2. What are the “Principles of Data Protection”?

These are the guiding conventions that everybody must work towards when processing other people’s personal information. The 6 key principles that we must all work towards are:

1. Personal data shall be:

    1. processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

    2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);

    3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

3. Responsibilities

Supervisory Authority

A Supervisory Authority is a public authority in an EU country responsible for monitoring compliance with GDPR. An EU country within the European Union is also referred to as a member state. A Supervisory Authority is typically a Privacy Commission or equivalent in a member state. It may have a different name in each country. For example, in the UK it is called the Information Commissioners Office.

The key role of the Supervisory Authority is to advise companies about GDPR, conduct audits on compliance with GDPR, address complaints from data subjects, and issue fines when companies are deliberately not complying with GDPR.

A Supervisory Authority is also referred to as a Data Protection Authority by some experts.

While a Supervisory Authority is responsible within a country, the companies operating in multiple countries may choose to appoint a Lead Supervisory Authority for the purpose of reporting. For example, the company should register the name of its DPO with the Lead Supervisory Authority. This can be a great simplification for companies that operate in multiple countries and choose not to appoint a DPO for each country of operation.

Controller

The controller is the natural person or legal entity that determines the purposes and means of the processing of personal data (e.g., when processing an employee's personal data, the employer is considered to be the controller). It is possible to have joint data controllers in certain circumstances. For example, when a company operates in multiple countries, but decisions on

processing purposes are being made both by central and local entities, the scenario would qualify as a joint controller.

The key responsibility of a controller is to be accountable, i.e., to take actions in line with GDPR, and to be able to explain the compliance with GDPR to data subjects and the Supervisory Authority, as and when required.

Processor

A natural person or legal entity that processes personal data on behalf of the controller (e.g., a call centres acting on behalf of its client) is considered to be a processor. At times, a processor is also called a third party.

The key responsibility of the processor is to ensure that conditions specified in the Data Processing Agreement signed with the controller are always met, and that obligations stated in GDPR are complied with.

Data Protection Officer (DPO)

The Data Protection Officer is a leadership role required by EU GDPR. This role exists within companies that process the personal data of EU citizens. A DPO is responsible for overseeing the data protection approach, strategy, and its implementation. In short, the DPO is responsible for GDPR compliance. It is possible that certain companies choose not to appoint a DPO, but assign the responsibility to an existing person in the organisation.

Normally, the choice of appointing a DPO, or not, is based on the scale of personal data that is processed in a company. For example, a small company that offers analytical services on medical records should have a DPO, because they process personal data, while a mid-sized manufacturing company may choose not to have a DPO, as the only personal data they process is that of staff and suppliers.

The key responsibility of the DPO is to ensure compliance with GDPR and advise company management and staff on the right measures to take.

4. Data Breach

A data breach is any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. If you discover that there has been a breach in security or personal information (pupil, teacher, governor or anybody else the school holds information on) has been lost or destroyed, you should report this via the use of a **PERSONAL DATA SECURITY BREACH REPORT FORM** (located at **Annex A** to this document) to the Trust Data Protection Officer.

Email: dpo@westnorfolkacademiestrust.co.uk
Tel: 01553 773393 Ext 280

Examples may include:

a. Access by an unauthorised third party

b. Sending personal data to an incorrect individual

c. Computing devices containing personal data being lost or stolen, e.g. USB stick

d. Alteration of personal data without permission

e. Loss of availability of personal data

Data Breach timescales

You must report a data breach **as soon as you discover it**. Once a breach is detected by anybody in the school, we have **72 hours** to inform the Information Commissioners Office.

Annex A to
General Data Protection Regulations Compliance Guidance

PERSONAL DATA SECURITY BREACH REPORT FORM

If you discover a personal data security breach, please notify your Head of Department immediately. Please complete this form and return it to the Data Protection Officer at dpo@westnorfolkacademiestrust.co.uk as soon as possible.

Question	Answer	Remarks
Date of breach:		
Date breach was discovered:		
Name of person reporting incident:		
Contact details of person reporting breach	Email: Phone:	
Brief description of personal data security breach:	Who was involved: What happened: Where did it take place: When did it take place: Why did it happen:	
Number of data subjects affected:		
Brief description of any action since breach was discovered:	What:	
Was incident reported to the Information Commissioner's Office (ICO):		
DPO USE ONLY		
Report received by:		
Date:		
Action:		
Date:		

Annex B to
General Data Protection Regulations Compliance Guidance

GDPR FREQUENTLY ASKED QUESTIONS

Can teachers still take pupil information (such as work books) home?

Yes. There is nothing to stop authorised school staff taking home information containing personal details, but it must be transported and held securely. It shouldn't be left unattended (in cars or with computer screens left on for non-authorised people to see) and if memory sticks are used, these should be encrypted.

Can I share information with people outside of the school?

This is still possible as long as the individuals in question are aware of their responsibilities regarding that data and we have authority to share the data. Sometimes data will be shared due to a legal obligation (safeguarding/child protection purposes) and this is fine as the GDPR provides a legal basis for this.

Other information is shared to enable the school to provide a statutory obligation and occasionally data will be shared to provide an additional service to staff or pupils. It is important that we know everybody who we share data with and they agree to sign a written document governing how data must be used, stored and ultimately returned to the school or destroyed after use.

If you are unsure whether data should be shared with an individual or other body, make sure the Data Protection Officer is made aware of your concerns (inform your head of school or data office manager).

Should I hide pupil names when sharing information with others outside of the Academy Trust?

If you can do so (or apply a code such as a serial number) without compromising the purpose of sharing the information, then this is a good method of restricting the risk to the individuals we hold data on.

This may be useful when meeting other teachers for the purposes of moderating marking practices. If you do not need to know the individuals in question, it is advisable to remove their details for this purpose.

Should I anonymise pupil information?

If you no longer need to identify individual pupils but wish to keep any aggregated data (for analysis) then completely anonymising the data (so that you can never re-identify the pupil in question) is a good idea as this removes the information from the scope of the GDPR. If you still need to identify the person in question, this won't be appropriate.

Should we have a clear desk policy?

This isn't an absolute requirement but any measures that could reduce the risk of loss or unauthorised access to personal information should be considered. If information is held on paper copies, always make sure it is locked away when not in use.

Can we put personal information on display boards?

Staff boards should not contain any sensitive information and as a general rule, all displays should contain no more information than necessary to fulfil the intended purpose of the notification board.

For pupil display boards, they should not contain any information that doesn't relate to pupil work or school activities and the wishes of parents.

How should exercise books that contain pupils' full names, and possibly photos, be stored in classrooms?

As pupils are likely to know the names of their peers, there is not a huge risk in leaving exercise books in view, as there isn't the potential for a hugely damaging security breach. That being said, it is good practice to store exercise books in a cupboard

Can we display pupils' photographs in school displays and include their full names?

Wherever possible, schools should avoid identifying pupils – if names are required, only first names should be used.

Photographs and videos taken by staff on school visits may be used for educational purposes, e.g. on displays or to illustrate the work of the school, where consent has been obtained

Can we display the photographs of school leavers and include their name?

Past pupil photographs can be used as part of a display if a school has a lawful basis for doing so, such as their consent; however, depending on the purpose of the use consented to prior to the photograph being taken, the individual's consent may need to be refreshed.

Do we need consent to print full names on leavers' hoodies?

As hoodies and other memorabilia do not fall under the usual activities of a school, schools could not rely upon the legitimate interests right to be able to process the data for that purpose and, as a result, consent would be needed.

Can we display pupils' work around school which includes their full name?

It is perfectly reasonable to display pupils' work around school and include their full name without consent.

Can we provide work that includes a pupil's full name to a company that are running a competition, without parental consent?

This does not fall under the usual activities of a school, so it would be good practice to apply pseudonymisation (anonymising the data as much as possible, e.g. blurring a photograph of a pupil) to the art work to reduce the risk of it being identified. If you are unable to use pseudonymisation, consent would be required.

What are the rules when writing about a pupil in a publication?

If it is for a legal publication, then schools should consider whether and why the name is needed. If it is for marketing, then schools should consider pseudonymisation – the individual has the right over what their identity is being used for, unless they have already given a blanket consent for marketing purposes

Are we able to display exam timetables in school?

Displaying exam timetables is a legitimate activity and way of communicating, so this is valid – consent is not required

Where do we stand on retweets from other organisations? Tweets may include pupil photographs, for example.

If consent has already been provided for use of an image on social media, the consent would cover retweets from other organisations.

Are images of pupils and staff considered personal data?

Images are considered to be personal data

How often do privacy notices need to be signed?

Consent should be kept under review and it should be refreshed if anything changes, so consent only needs to be sought once, unless anything changes.

Are separate privacy notices needed for parents?

If a privacy notice is intended for pupils and their families, it would be appropriate to outline how a school uses parents' information within this privacy notice – a separate privacy notice would not be required.

Do privacy notices need to be published on the school website?

Privacy notices must be communicated to data subjects to satisfy their right to be informed.

Who can be a school's data protection officer (DPO)?

The role of DPO can be undertaken by an internal or external individual, as long as they have professional experience and knowledge of data protection law.

How can we ensure our suppliers are compliant with the GDPR?

There is no set criteria for proving compliance with the GDPR – you should review their relevant policies and procedures, however, and ensure their processes are in line with the GDPR.

Can I do a disc of photos for my Year as a leaving gift? Photos have been used for newsletters etc... No names are on any of them.

Yes, as long as you get consent from parents, those involved.

We can rely on consent collected for use of the original photos/videos as long as popping them onto a disc for this purpose is seen as compatible to the original request for permission (it would have to include publication of the images) but if they've all been used (with adequate consent) for newsletter, this should be fine.

What if I have further questions?

Pass these on to your head of school/Department do simply contact the Data Protection Officer who will provide advice as required.
Email: dpo@westnorfolkacademiestrust.co.uk
Tel: 01553 773393