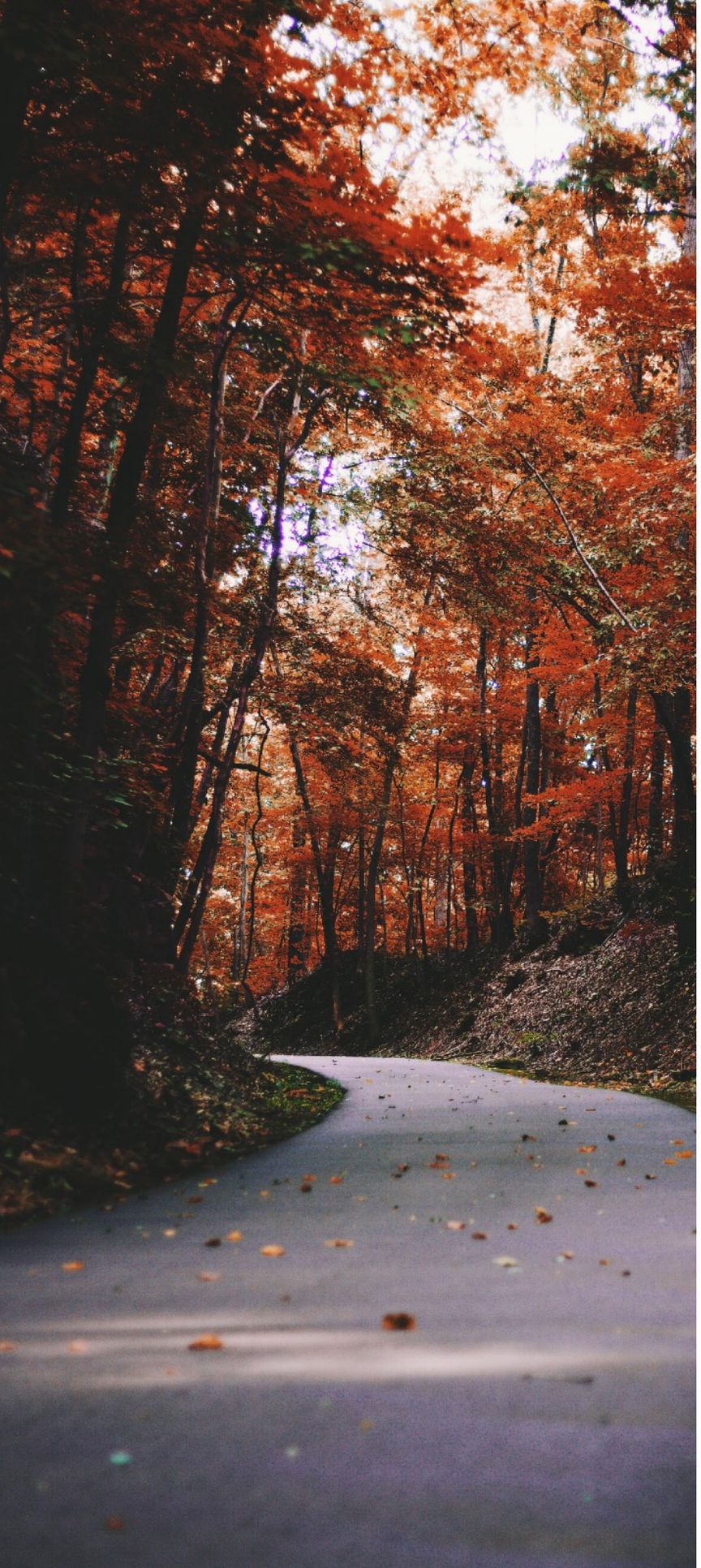
e4education

Our Guide to GDPR

CONTENTS



WHAT IS GDPR?

The General Data Protection Regulation (GDPR) will become law on the 25th May 2018 and replaces the outdated Data Protection Act 1998 (DPA). The European Parliament, Council of European Union and European Commission have brought about this change to strengthen and modernise data protection for individuals within the European Union (EU). Although driven by the EU, GDPR will still apply post-Brexit.

Let's take a look at some terminology and show you what we are doing to ensure our products and service are GDPR compliant.

DATA SUBJECT

Data subject means an individual who is the subject of personal data. The personal information of deceased persons is not protected. Examples of a data subject:

- You
- Another staff member
- Pupil

PERSONAL DATA

This regulation is all about personal data. GDPR states that personal data is:

"ANY INFORMATION RELATING TO AN IDENTIFIED OR IDENTIFIABLE NATURAL PERSON (DATA SUBJECT)"

Examples of personal data:

- Name
- Email address
- Telephone number
- Address
- Date of birth
- Your IP address

PROCESSING DATA

When it comes to processing data, this is deemed to be any operation or set of operations performed on personal data. Examples of processing data:

- Usage
- Collecting
- Organising
- Recording
- Storage
- Destructing

DATA CONTROLLER (SCHOOL)

Under GDPR, schools or organisations who decide the purpose and means of processing personal data are considered to be Data Controllers. Schools in Scotland are the exception to this where Data Controllers are the local authority.

GDPR states that the Data Controller shall:

"BE RESPONSIBLE FOR, AND BE ABLE TO DEMONSTRATE, COMPLIANCE WITH THE PRINCIPLES."

DATA PROCESSOR (E4EDUCATION)

A Data Processor is a person or organisation that processes data on behalf of the Data Controller. In education, a Data Processor would be a third-party supplier that uses pupil, parent or staff personal data to provide the school with services or products. Examples of data processor:

- MIS provider
- Library system supplier
- Website provider
- Cashless catering system

WHAT OBLIGATIONS DO DATA CONTROLLERS AND DATA PROCESSORS HAVE?

Data Controllers are obligated to determine:

- The legal basis for collecting data
- Which items of personal data to collect
- The purpose(s) the data is to be used for
- Which individuals to collect data about
- Whether to disclose the data and, if so, to whom
- Whether subject access and other individual's rights apply
- How long to retain the data

Data Processors have obligations too, which must be set out in a legal contract:

- Processes the personal data only on documented instructions from the controller
- Ensures their staff involved in processing the data observe confidentiality
- Takes appropriate security measures to protect the data
- Helps the Data Controller by using appropriate technical and organisational measures
- Helps the Controller to ensure compliance
- Returns or deletes all the data a the end of the contract
- Provides the controller with all information necessary to demonstrate compliance

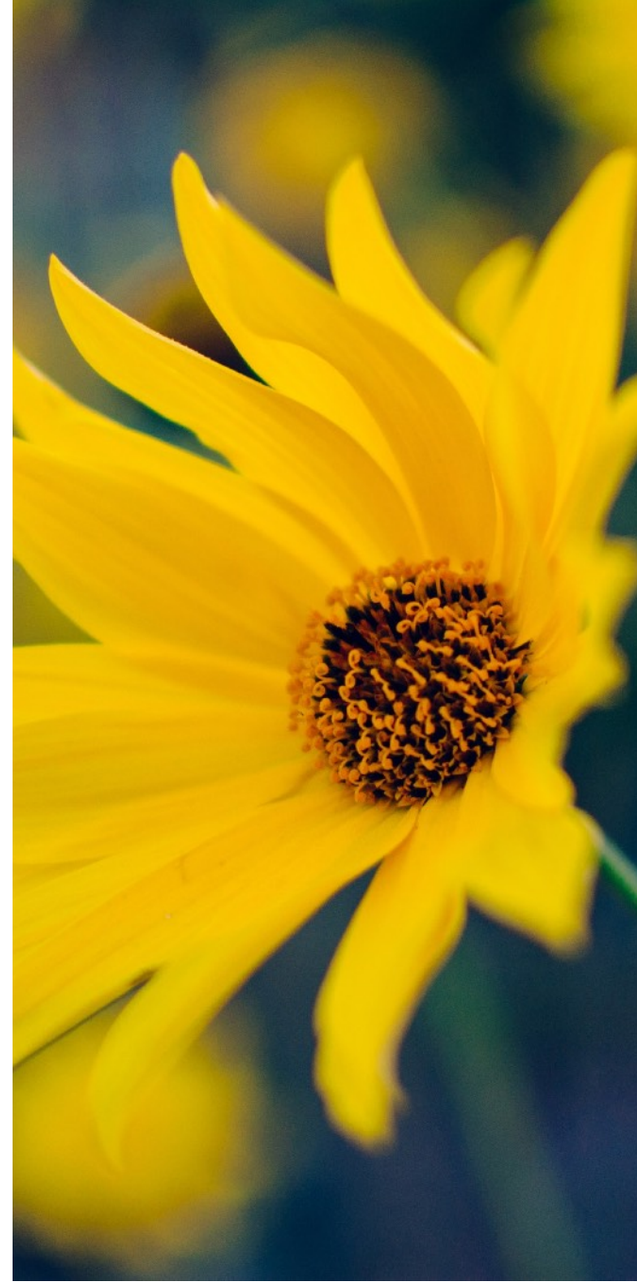
The controller shall take appropriate measures to provide information relating to processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language...

GDPR Article 12-1

KEY DIFFERENCES BETWEEN GDPR AND DPA

Appointment of a Data Protection Officer (DPO)

This person is responsible for advising and guiding the organisation and is a point of contact for all data subjects and the Information Commissions Office (ICO).



Increased accountability and governance

Higher expectations on organisations to put measures in place to enhance data protection and minimise the risks of personal data being breached.

Enhanced rights of individuals (data subjects)

The GDPR places the rights of data subjects and their personal data at its core.

It will be a law

The DPA is part of a directive, whereas the GDPR will be a law.

The age of data consent will be 13

Under GDPR, processing a child's personal data is lawful where the child is at least 16 years old and has given consent. However, member states can change this. The UK have agreed that the age of data consent will be 13.

THE SIX PRINCIPLES OF GDPR

In short, the principles ensure you only collect the data you need, you explain why you are collecting it and who you share it with. The data is kept up to date, secure and retained for only as long as it is needed.

1. **Processed fairly, lawfully and in a transparent manner**
   There must be a genuine reason, known as a lawful basis for processing the data and you must explain this to the data subjects at the time of collection. This is done in a privacy notice, written in a way that they understand.

2. **Collected for specified, explicit and legitimate purposes**
   Being clear about the reason for collection, means that you won't do anything else with the data at a later stage without explaining it to the data subjects.

3. **Used in a way that is adequate, relevant and limited**
   This is about data minimisation, only collecting the data that you need. Asking yourself why you need the data and how you are going to use it. This will expose any data that you don't need to collect. Remembering, you can't collect data just in case you might need it in the future.

4. **Processed in a manner that ensures appropriate security of the data**
   You must take reasonable steps to secure personal data, both technically and physically. This includes appointing somebody with responsibility for data security, training staff, reducing the risk of data breaches, such as by encrypting memory sticks, emails and implementing processes so that you quickly respond to security incidents.

5. **Kept no longer than is necessary**
   Part of your data mapping exercise, the process of accessing all existing and future systems should address how long you need to keep data you hold. If you are holding it for longer than you need, consider why and whether it can be securely deleted or destroyed. This includes old paper files and electronic backups.

6. **Processed in a manner that ensures appropriate security of the data**
   You must take reasonable steps to secure personal data, both technically and physically. This includes appointing somebody with responsibility for data security, training staff, reducing the risk of data breaches, such as by encrypting memory sticks, emails and implementing processes so that you quickly respond to security incidents.

The key reason for the GDPR is to strengthen the rights of individuals and to prevent organisations misusing personal data. Under the GDPR, individuals have a right to be informed about the data you hold on them, why you hold it and what you do with it.

RIGHTS OF DATA SUBJECTS

- **The right to be informed**
  Explaining what information you hold on individuals, where it came from and what you will do with it, is typically explained in privacy notices. Under the GDPR, this must be clear, concise and written in a way that the data subject will understand. Being transparent from the outset will help reduce potential objections to processing.

- **The right of access**
  Individuals have the right to access their personal data and confirm the lawfulness of processing. This can be done through a Subject Access Request. This is already possible under the DPA but the GDPR tightens up the reasons individuals can make these requests and specifies that organisations should reply within 1 month.

- **The right to rectification**
  Data subjects must be able to inform you when their data changes or be able to correct it themselves. You must also update any data you have shared with third parties.

- **The right to object**
  Individuals can object to their data being processed for purposes such as direct marketing.

- **The right to restrict processing**
  The data subject has the right to restrict processing of their personal data if it is inaccurate. The data subject may object to the erasure of data but still allow you to restrict processing instead. This wouldn't apply if there is a statutory or contractual purpose for processing the data. However, you must make clear your reasoning behind processing personal data.

- **Rights in relation to automated decision making and profiling**
  A data subject has the right not to be subjected to a decision based solely on automated processes, without human intervention. An example of this could be an online aptitude test or application for a loan. You are only allowed to use this type of decision making if, the data subject has given their explicit consent, it is necessary to perform a contract or it is authorised by law.

- **The right to data portability (New)**
  This is to help individuals easily move from one IT system to another, in a safe and secure way.

- **The right to be forgotten (New)**
  If you need the data for statutory purposes, you do not need to delete it. If it is no longer required, then it should be removed. The regulation does not apply to the personal data of deceased people.

- **The right to access personal data held**
  This is called a Subject Access Request and is discussed in detail on the next page.

SUBJECT ACCESS REQUESTS

Just like the Data Protection Act, data subjects have the right to request information that is held on them. This is known as a subject access request.

GDPR stipulates that Subject Access Requests:

- Have to be dealt with in one month, including weekends and bank holidays.
- Must be acknowledged and reported as soon as possible.
- Staff must recognise and know what to do when a Subject Access Request comes in. This could be verbal, a letter or by electronic means.
- A data subject can ask for more clarity or to narrow the request if large volumes of data is supplied.
- The request must be validated. It is recommended that a request is confirmed in writing and identification is gained.
- You are no longer able to charge for a Subject Access Request, though further copies may incur a reasonable admin fee.
- You should have a Subject Access Request procedure in place, which includes a central record of all requests made. A member of staff, usually the Data Protection Officer should be trained in handling Subject Access Requests.
- You may be required to retrieve information under your control (e.g. in your email) relating to the Subject Access Request. Therefore, only keep information for as long as it is required.
- It is a criminal offence to alter data in response to a Subject Data Request.

DATA BREACHES

What is a data breach as defined by the GDPR?

"A BREACH OF SECURITY LEADING TO THE DESTRUCTION, LOSS, ALTERATION, UNAUTHORISED DISCLOSURE OF, OR ACCESS TO, PERSONAL DATA TRANSMITTED, STORED OR OTHERWISE PROCESSED".

It's important to note that a breach is more than just losing personal data. It also covers:

- **Destruction**
  Where the data no longer exists or no longer exists in a form which is of any use to the organisation.

- **Damage**
  Where personal data has been altered, corrupted or is no longer complete.

- **Loss**
  Losing control or access to it or no longer having it in your possession.

- **Unauthorised or unlawful processing**
  This could include exposure of personal data to third parties who are not authorised to access the data.

HANDLING A DATA BREACH

All organisations should have a data breach procedure in place. It's important you know what to do in the unfortunate event that a data breach occurs. You may not be responsible for managing a data breach but you must know what to do if you become aware of one.

YOU MUST NOTIFY A BREACH TO THE ICO WITHIN 72 HOURS, UNLESS IT IS UNLIKELY TO RESULT IN A RISK TO THE RIGHTS AND FREEDOMS OF INDIVIDUALS.

Data breaches could be caused by a number of factors. Some examples of these might be:

- Loss or theft of data
- Loss or theft of actual device/equipment on which data is stored e.g. a memory stick
- Inappropriate access to controlled areas or rooms
- Human error e.g. sending information to the wrong person

A member of staff, usually the Data Protection Officer, should be trained in handling data breaches. It’s important to know who this person is.

IMPLICATIONS OF A DATA BREACH

If a data breach is not handled in accordance with GDPR, you may receive a fine. The fine you receive will be dependent on the type of breach you have.

At the discretion of the governing body, fines could be as much as:

- €10 million or 2% of turnover (whichever is higher)

For issues surrounding consent, data security, communication of breaches to data subjects and the ICO.

- €20 million or 4% of turnover (whichever is higher)

For issues surrounding conditions of consent, processing sensitive categories of personal data, data subjects rights and the lawfulness of processing.

These are maximum level fines. However, it is crucial to recognise the importance of compliance within the new GDPR.

WHAT CAN YOU DO TO COMPLY?

Schools are required to identify all categories of data held about students, parents and staff, the purpose for which the data is being held and how it is being processed. By doing this, you will become familiar with the personal data ecosystem within the school.

Once identified, this information can be used to run an audit. To assist, the ICO have developed “Data protection self-assessment” tool which rates your current practice and gives a clear indication as to where your strengths and improvements are.

Data protection self-assessment tool:

https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/

Here are a few tips for keeping personal data safe online:

- Encrypt data or use password protection features where possible.
- Do not email personal information to your personal email address.
- Do not store personal data on your own phone or device, unless the school has approved doing so.
- Be careful that your emails go to the person they are intended for.
- Only copy emails to people that really need to see them.
- Delete emails that you no longer need.
- Use strong passwords and change them regularly.
- Ensure you log out of shared devices.
- Do not carry information around on memory sticks, unless it's encrypted.
- Make sure electronic data is destroyed correctly.
- If your department has purchased any new software, ensure your Data Protection Officer and IT department are informed.

WHAT CAN YOU DO TO COMPLY?

When you're not online, you may like to consider the below for keeping personal data safe:

- Proper disposal of paper files.
- Looking after or supervising visitors on site.
- Keeping laptops or other devices secure when they're not in use.
- Be careful about the paperwork you carry with you each day.
- Only print out information if it is completely necessary and keep it safe.
- Don't leave important documents on a photocopier or in a printer.
- Keep devices or documents locked away when not in use.
- Shred or securely dispose of personal data once you have finished with it.
- Check any suppliers you use comply with necessary regulations.

Other things to think about:

- For the use of CCTV in and around the school, you will have a policy in place. It's important that you read and understand it.
- You should appoint a Data Protection Officer.
- For services provided directly to children, it's important that your privacy policy is really clear and written in a way that a child would be able to understand.

‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

GDPR Article 4-6

WHAT HAVE WE DONE TO HELP YOU COMPLY?

Developing beautiful websites with best practice and data protection by design, has always been at the forefront of our thoughts. We have been working diligently to incorporate new data protection elements within our products and services to assist you with GDPR compliance. GDPR functionality will be available to 4.5 clients at the end of April 2018.

CHANGES TO YOUR WEBSITE ADMIN TOOL (4.5 CONTENT MANAGEMENT SYSTEM)

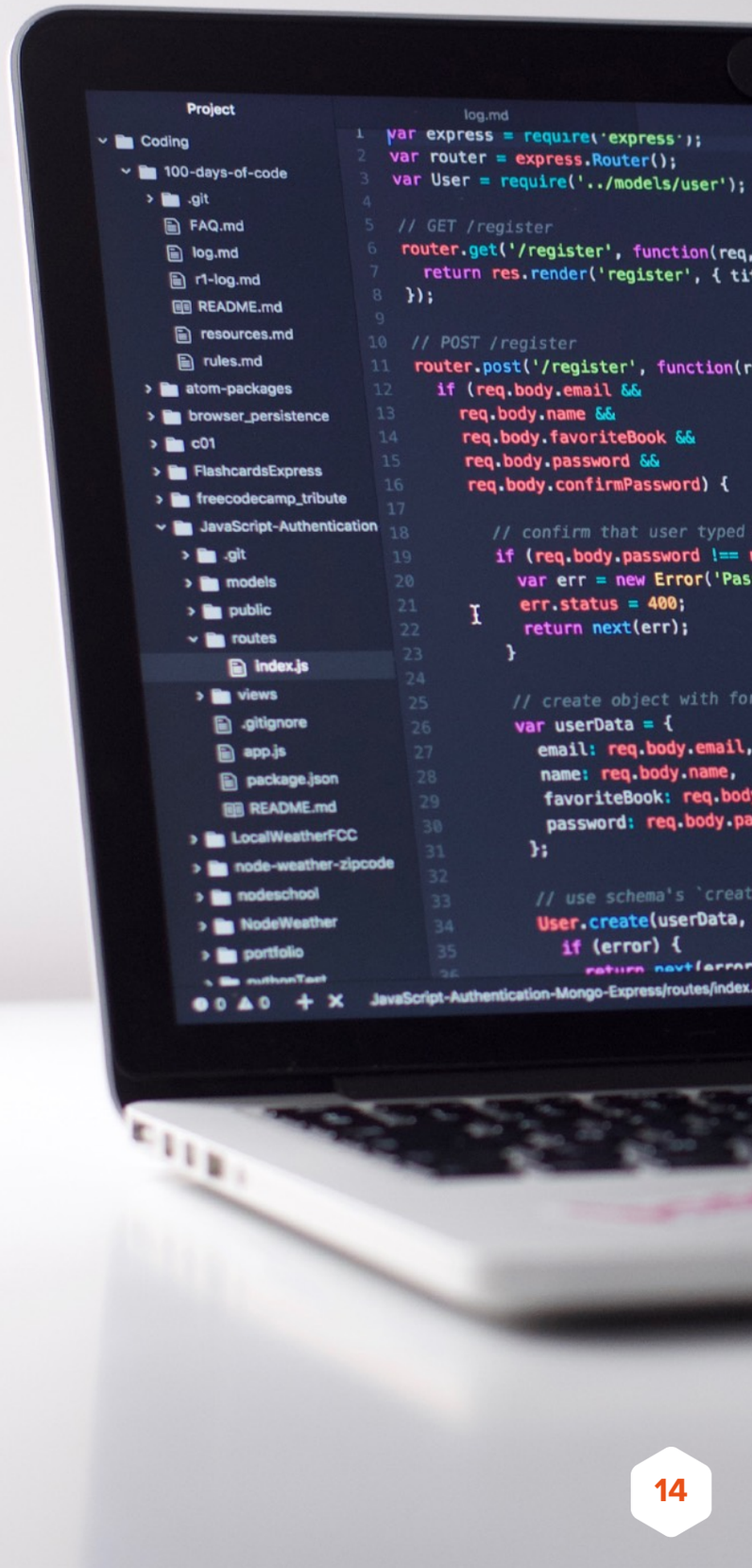
USER MANAGER

As staff leave or join the school, it is important to keep on top of their website user accounts. Not only for reasons of security but to ensure the accuracy of their personal data and to delete that data if it is no longer required. This is detailed in points 4 and 5 of the GDPR principles. To help you manage that data we have developed the following:

- A user with appropriate permissions will receive an email notification when other users of the website have not logged into, or updated their account after a set period of time.

- A new Data Protection Officer (DPO) role will appear in the User Manager. This role should be allocated to a member of staff within the school. They will then receive data protection emails, generated by the website and any items requiring action will appear in their review queue. If the DPO user is changed, outstanding items will be transferred to the new DPO user.

- Deleting a user account will completely strip their personal data from the website.



WHAT HAVE WE DONE TO HELP YOU COMPLY?

FORMS

To help ensure you retain personal data obtained from forms, for only as long as it is required, you can now:

- Remove form submissions in bulk, rather than individually. Once marked as removed, this data will no longer be accessible via the website admin. However, submissions will still exist within the websites database. A scheduled process on our servers will run overnight to permanently delete any submissions marked as "removed" from the website database. This gives you a little grace period to retrieve the data via our Support Team, just in case it was accidentally removed.

- If a form is deleted from the website, we will automatically and permanently delete any associated form submissions.

- Form submissions will now be encrypted in the websites database by default.

COOKIES

Cookies are generally used to track visitors movements across a website, how long they spent on a page, links clicked, preferences for layouts, colour schemes and much more. GDPR now forces the importance of obtaining consent when collecting personal data. You must document in a Privacy Policy the cookies used, what data they are gathering and where they are coming from.

- We are giving you the ability to enable or disable a cookies message. You can select whether you prefer it to appear as a bar or pop-up. You can also select colours for the text, background and position. Before applying the cookies message, you can view how it looks in a nifty preview window.

- The cookies message will no longer assume implied consent. It will ask if the visitor would like to:

1. **Accept cookies**
   The site will display as normal and cookies will be allowed.

2. **Don't accept cookies and remember my choice**
   Visitors will have an option to save a cookie to remember their opt out choice. The website will display with fallbacks for areas that require cookies.

   For example, if your school website has a Google map at the bottom, this requires the use of Google cookies. A fallback option here could be to display some default text or to have something designed by our team.
   Please note, if you would like something specific designed as a fallback option, this will be quoted accordingly.

3. **Don't accept cookies and don't remember my choice**
   If this option is selected, the cookies message will always display. The website will display with fallbacks for areas that require cookies.

WHAT HAVE WE DONE TO HELP YOU COMPLY?

COOKIES CONTINUED

- A link will be added to the footer of your schools website. This link will allow those users who opted out of cookies a means to opt in.

- Enabling the cookies functionality will scan the entire website for the use of cookies. Cookie usage could form part of the design or it could come from embedded content e.g. if a member of staff embeds a YouTube video within the content area. YouTube uses cookies and because the content has been embedded on the website, YouTube cookies will be active.

If it has been identified that cookies exist and they are not listed on the Privacy Policy, the Data Protection Officer will receive an email notification with a list of those cookies. This user should then update the Privacy Policy with information about who these cookies come from and what they're doing.

YOUR WEBSITE DATA

In the unfortunate circumstance that you decide to leave e4education, we want you to know that we still care about protecting your schools personal data. To comply with GDPR we have put measures in place to dispose of personal data within the User Manager and completely clear form submissions from your website. We will retain a copy of your website, excluding any personal data, for 3 months after you leave, just in case you need the content or design.

PARTNERED WITH GDPR.CO.UK

A great, centralised tool for ensuring you remain on top of your GDPR compliance within the school. For more information and an idea of costs, feel free to contact our Sales team.

PRIVACY POLICY TEMPLATE

Where personal data is processed, it's important that you explain what data is processed, how it is processed and why it is processed in a detailed Privacy Policy. To give you a little guidance, we have put together an example Privacy Policy. If you would like to use this example, please read it carefully and modify it to fit your schools website.

http://resources.e4education.co.uk/gdpr/example_privacy_policy.pdf

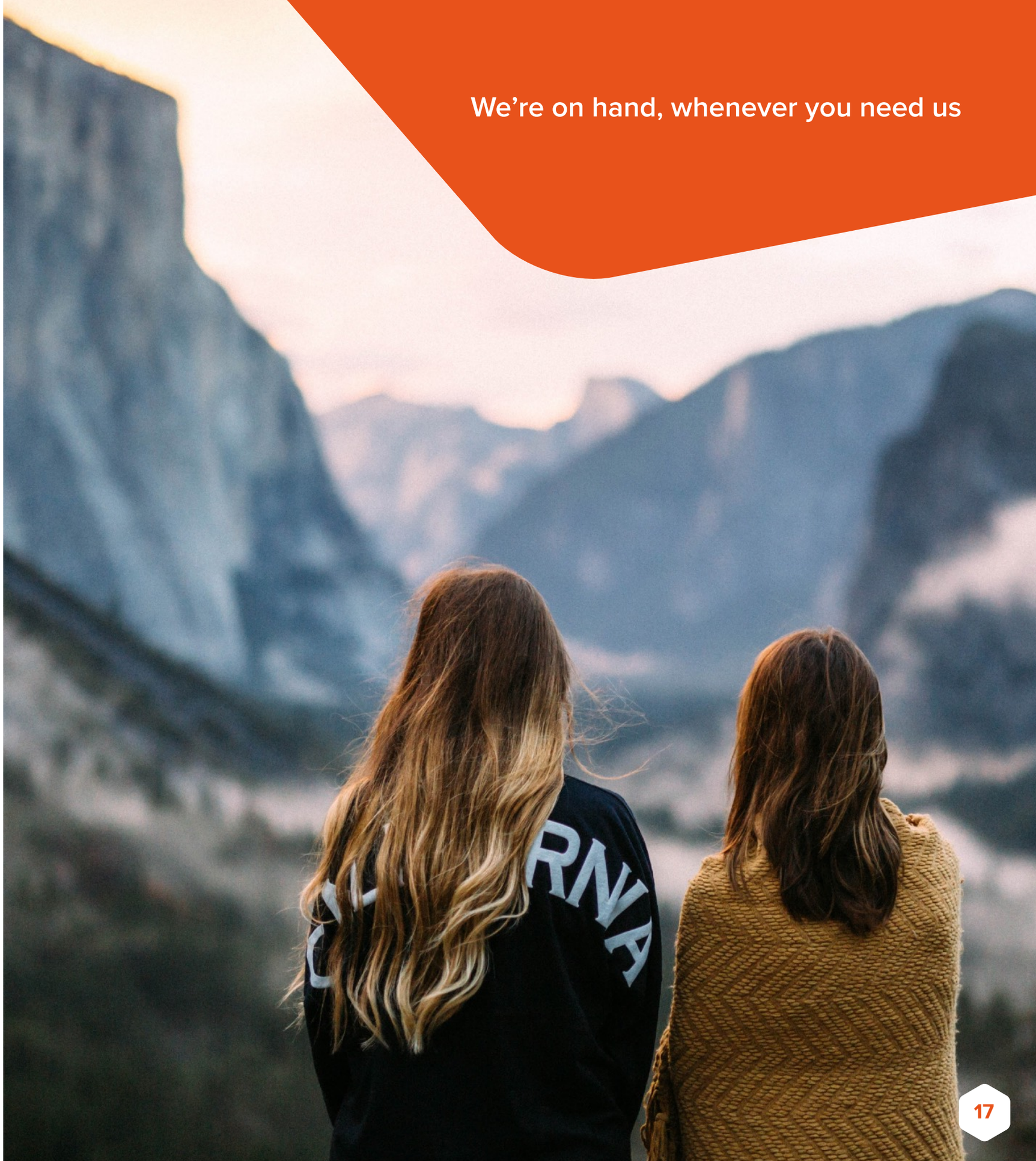
A CHANGE TO OUR SUPPORT PROCEDURE

It’s important to ensure that when calling our Support team, change requests are raised by valid users with appropriate permissions.

To validate users over the telephone, above and beyond a username, school name and email address confirmation, we are implementing **Support Codes**.

When you call our Support team for assistance, you may be asked to provide a code. The code is available under the Help tab and continually updates. Once clicked, the Support Operative will see the code and ask you to confirm this over the telephone before proceeding with your request.

We understand that an additional step in actioning your request may seem laborious but we really do have your best interest at heart. We care about your website security and do our utmost to prevent misuse.



SECURITY

What happens when a visitor views your website?

Visitor Device
The schools website address is entered in to a browser. For a faster load time, a request is sent to the varnish server. The varnish server will store a copy of public facing pages, also known as cache.

Varnish Server (London)
If the varnish server has a cached page stored, it will send this back to the visitors device. If it does not, it will request a fresh copy from the website server. The physical websites files and database are situated on the website server.
Content you cannot see via the public facing website is not cached. For example, the file manager (where a file has not been linked to a public page), user manager and form submission data.

Website Server (London)
Content on your schools website is hosted by Rackspace at their London data centre. Rackspace looks after the server your site sits on and ensures it is secure, up to date, backed up for the purposes of disaster recovery and provides hardware replacement if necessary.
Rackspace operates a dedicated Customer Security Operations Centre, which is staffed 24x7x365 by certified security analysts. They detect and provide rapid response to threats, performing remediation to quickly ensure things are back up and running, should anything terrible happen.

OLDER WEBSITE CMS CONSIDERATIONS

If your school website is running on an older version of our admin tool (CMS), unfortunately you will not have access to our latest GDPR technology. However, we have listed some things for you to consider for GDPR compliance below:

- Are you using forms to obtain personal data on your website?
  - ☐ If so, have you included a consent checkbox?
- How long are you retaining form submissions?
  - ☐ Providing you have sufficient permissions, you will have the means to delete form submissions from your website. You should ensure that form submissions are kept for no longer than is required for the task or activity.
  - ☐ Deleting form submissions can be achieved in different ways, dependent on your website version. If you are unsure, contact our Support team who will walk you through this process.
- Are your users up to date?
  - ☐ Check your User Manager to ensure all users are still actively employed by the school. If someone has left, delete their account.
  - ☐ Ensure all active users have their own account.

If you haven't already, why not book a demo of our latest CMS. Quote E4E-GDPR to receive a 50% discount when purchasing an upgrade before May 2018

OLDER WEBSITE CMS CONSIDERATIONS

- Do you know if your website uses Cookies?
  - ☐ Cookies could form part of the design. For example, does your website have a YouTube video on the homepage slideshow? If it does, the website will pull through YouTubes required Cookies.
  - ☐ Are those users with relevant permissions, embedding third party content to various areas of the website? This could include embedded content, such as YouTube, Vimeo, Google Maps, etc
  - ☐ If you are unsure of how to check for the presence of Cookies, contact our Support team who will check this out for you! If you have a number of users updating website content on a regular basis, it's important to regularly run a cookies check.
- If Cookies exist, do you have a cookies bar or popup message?
  - ☐ Dependent on your website version, you may or may not have the means to incorporate a Cookies message. Contact our Support team for more information.
- If Cookies exist and you have a Cookies message, do you have a Privacy Policy somewhere on the website?
  - ☐ If you do not have a Privacy Policy on the website, we have put together a template to get you started. You should include information about Cookies relevant to your website.
  - ☐ As your website content grows, you should regularly schedule a review of your Privacy Policy to ensure it is up to date.and accurate.

If you haven't already, why not book a demo of our latest CMS. Quote E4E-GDPR to receive a 50% discount when purchasing an upgrade before May 2018

e4education

IF YOU REQUIRE ANY MORE HELP OR ADVICE, PLEASE GET IN TOUCH.

03453 191 039

@e4education

help.e4education.co.uk