THE DEFINITIVE GUIDE TO THE GENERAL DATA PROTECTION REGULATION

Sprint Education

The GDPR's Impact on Marketing to Schools

How your education business will be affected, what Sprint Education has done, and what you need to do.

Including!
Learn how to spot marketing agencies that don't comply, or that disclose misleading GDPR guidance.

Sprint Education...

Is an award-winning digital agency that has pioneered digital and inbound marketing to the UK education sector since 2007.

We create over 48 million teacher connections for our clients every year through delightful digital marketing plans and our education marketing and sales software (Campus) that attracts teachers, school staff, and educational establishments to our clients' brands.

This report was written by Guy.

"I co-founded Sprint Education back in 2007, and since then I've learnt so much about our industry and the inner-workings of communicating with the education sector. Many of you will know that I was once a teacher myself, and so know all about the pitfalls education businesses must avoid when it comes to choosing an education agency to manage their marketing. **This is going to become even more important in light of the GDPR**.

I've written this report to help guide you towards **GDPR compliance** and to give you an overview of what we've done to ensure its own compliance."

Guy Lewis
Co-Founder – Sprint Education
guy@sprint-education.co.uk

Contents

Please note that this guide is for informational purposes only, and should not be relied on as legal advice. You should work with legal and other professional bodies to understand exactly how the GDPR might apply to your organisation.

I wrote this guide to explain specifically how the GDPR will impact marketing to schools and teachers; to share some of what we've done at Sprint to meet the stringent requirements; to explain how it will affect our education communication services going forward; and to outline some things you can do to help you in your quest for compliance.

I didn't set out to write just another GDPR guide that covers every aspect of the new legislation – there are tonnes of articles out there that will tell you what it is. Some are good and written by legal experts; some are bad and written by people who have clearly not taken the time to actually read the regulation. I've even come across a couple of agencies recently who claim to be marketing to school experts and who have publically stated **MASSIVE** inaccuracies and legal misconceptions like:

"You must be able to show that every teacher on your marketing list has given consent."

This is plain **WRONG**; there are other legal grounds for processing personal data. Even the Information Commissioner at the time of the GDPR being introduced, Elizabeth Denham, called out these doom-mongers as pedalling 'fake news'. You can read more about Sprint Education's legal ground for processing teacher personal data on page 14of this guide.

"Email campaigns don't work well and will quickly fall foul of the GDPR."

WRONG again. Emails work really well when you have experts managing them for you, and as for "falling foul of the GDPR", that's just nonsense. As long as you take measures to ensure you're doing it legally there's no problem (more about how Sprint's Managed Email Service does comply on pages 17 and 18).

My advice is to look carefully at the services that these agencies offer and ask yourself the question, "What do they have to gain from not giving me the full picture?"

You can read more about common misconceptions that people have in Chapter Two, which starts on page 7.

As the disclaimer says above, I am not a legal expert but I have read the regulation, several times, obsessed over it, discussed it with legal experts, and, well, basically lived and breathed it for the last two years. I should impress though that there really is no better resource than the regulation itself (all 54,876 words of it). So, if you deal with data at your organisation I would recommend this guide is used as a springboard to you reading the real thing.

Okay, let's get started!

Chapter One:
About the GDPR

What is it?

The EU's General Data Protection Regulation (GDPR for short) is the result of several years' work by the EU. It was adopted in April 2016 by all EU Member States (including the UK) and became enforceable law on 25th May 2018.

The EU created the GDPR for two main reasons.

Firstly, they wanted to bring the laws surrounding data protection in line with our modern world.

In the UK we previously were governed by a set of laws called the Data Protection Act (DPA for short) from back in the 90's that was created before the emergence of cloud providers and internet giants like Google and Facebook. The GDPR was brought in to stop data being exploited, and strengthens and protects all of our rights.

Secondly, the EU wanted to simplify and standardise the approach to data protection across its member states.

This is so that businesses have a simpler and unified way of dealing with data.

Failure to comply with the GDPR can result in hefty fines, which can reach as high as €20 Million or 4% of global annual turnover, whichever is higher.

And, just a note on Brexit: Because the GDPR came into force before the UK's official exit from the EU, the regulation does stand. Even now the UK has left the EU, the new Data Protection Bill that the Government published in September 2017 does contain the same high standards of data protection that the GDPR does. So if you haven't already, now is the time to get your house in order and get compliant.

Who is affected?

People and organisations, basically.

Millions of EU citizens will ultimately benefit from the more stringent data protection measures that the GDPR sets out, and any organisation in the world, if they hold and process any personal data of EU citizens, must also abide by the law.

Within these organisations, there are two demographics who are be most affected. They are called 'Data Controllers' and 'Data Processors'.

Data Controllers state how and why data is processed and make decisions surrounding it. If you collect leads through a lead generation form on your website to grow your marketing list, you are the Data Controller of that data.

Data Processors process the data according to the Data Controller's wishes. The provider of the CRM that you just dropped your collected lead generation data into is the Data Processor.

It's the controller's responsibility to ensure that their processor abides by data protection law –but processors don't get off lightly; they have to abide by GDPR rules too.

What is 'personal data'?

Personal data is any information related to a natural person or 'data subject' that can be used to directly or indirectly identify the person. It includes their name, their email, even online identifiers like their IP address.

What does it mean to 'process data'?

Processing data is any operation performed on the data, such as collecting it, storing it, editing it, using it for marketing, etc.

What responsibilities do organisations that process personal data have?

Put simply, controllers must ensure that personal data is:

- processed lawfully (there are six lawful grounds they can rely on to do this)
- collected for specified, explicit and legitimate purposes
- accurate and kept up to date
- not kept for longer than is necessary
- kept securely

The controller also needs to be able to demonstrate their compliance with these principles.

How did responsibilities change?

The GDPR extends many principles from the old directive that it is replacing, and sets a higher bar with several ambitious changes:

1. Expansion of scope

The GDPR applies to any organisation that processes the personal data of any EU citizen; even if that organisation is based outside the EU.

2. Tighter definitions of personal and sensitive data

The GDPR covers traditional personal data like names, addresses, and emails, but also new types of data like IP addresses, behavioural data, biometric, financial, and even 'pseudonymised` personal data.

3. Greater rights to individuals

Amongst other rights, individuals will have the right to be forgotten, the right to object to processing, the right to rectification, a right to access the data you process on them, and the right of data portability.

4. Much stricter consent requirements

Many organisations will find the consent that they obtained from individuals to process their data pre-GDPR will no longer be considered consent under the GDPR, and will need to gain new consent under the new rules. We'll look at consent in more detail later.

5. Much stricter processing requirements

Individuals now have a right to receive 'fair and transparent' information about the processing of their data, which includes being told who the data controller is, why the data is being processed, how long the data will be held, and the legal ground under which it is being processed.

There are many other responsibilities under the GDPR so make sure you review the text of it carefully.

Chapter Two:
The GDPR and Marketing to Schools

There's plenty of good (and very bad) advice out there about the GDPR but nobody's explained how it's going to affect marketing to schools. Many of our clients have been looking to us and asking how it will affect them, and also how it might affect the use of our services going forward.

Before we look at how marketing to teachers at schools will change under the GDPR, it's important to understand where we're coming from. So let's first look at how it works currently, pre-GDPR.

Before the GDPR

Every organisation that sells to schools and teachers (and abides by the law) currently processes personal data, and uses that data for marketing purposes to teachers at their school work addresses using two complementary pieces of legislation:

The DPA

(The UK's Data Protection Act, 1998)

This implements the EU's Data Protection Directive 1995, and is the legislation that the GDPR is updating. It is based around eight principles of good information handling which give people specific rights in relation to their personal information and places certain obligations on those organisations that are responsible for processing it.

Not unlike the GDPR, if direct marketing involves the processing of personal data (in simple terms, if the organisation knows the name of the person it is contacting), it must comply with the principles set out in the DPA.

PECR

(The UK's Privacy and Electronic Communications Regulations, 2003)

This implements the EU's European Directive 2002/58/EC (which is also known as the ePrivacy Directive). PECR works alongside the DPA and just sets out some extra rules for electronic communications (like email marketing).

Put them together and the DPA ensures that organisations process data legally, while PECR sets out further rules on how that data is treated when being used specifically for electronic marketing.

A common misconception

Now you may have read that, under PECR, email marketing requires the consent of the person for it to be legal, and you'd be right – if you were applying that to consumers, sole traders, or partnerships outside Scotland.

Schools (and their employees) are not covered under this part of the law, and the Information Commissioner's Office (the enforcers of the DPA and PECR) are very clear on this. They say:

"The rules on consent, the soft opt-in, and the right to opt out do not apply to electronic marketing messages sent to 'corporate subscribers' which are defined as companies and other corporate bodies e.g. limited liability partnerships, Scottish partnerships, and government bodies. The only requirement is that the sender must identify itself and provide contact details."

To elaborate on this a little: State schools are considered government bodies, and schools in the private sector hold limited liability, and are therefore considered corporate bodies. Teachers at the schools are considered 'users' (which is a term used to describe any individual using the electronic communications service e.g. phone or internet connection owned by the corporate subscriber).

In addition, the ICO goes on to say:

"Many employees have personal corporate email addresses (e.g. firstname.lastname@org.co.uk), and individual employees will have a right under section 11 of the DPA to stop any marketing being sent to that type of email address."

So, to distil all that down into simple terms: Under current legislation, marketing via email to teachers at schools is perfectly legal as long as you abide by everything else in both the DPA and PECR.

After the GDPR

Fundamentally, the actual mechanics of marketing to schools and teachers under the GDPR and PECR will not change a great deal. Schools will continue to be 'corporate subscribers', teachers and school staff will remain their 'users', and consent will still not be a requirement*, as long as another one of the GDPR's legal grounds for processing personal data is met. Despite this, meeting the new stringent obligations surrounding the processing of personal data that the GDPR sets out will be a significant challenge for many education suppliers.

*I should note here that whilst marketing to schools and teachers under the GDPR and PECR will not necessarily require consent, the EU is currently working on a new ePrivacy Regulation which is currently in draft form which

may change things. However, until this is agreed by the EU Council of Ministers and EU Parliament, we cannot assume that it will. We're keeping a very close eye on the development of this and will publish our thoughts as and when the EU's position is clear.

Key GDPR changes

The GDPR improves upon the DPA legislation and gives data subjects more power. As an education supplier, you'll no doubt process personal data of some kind (e.g. a list of teachers in your CRM who have bought or enquired from you in the past) so we've selected some of the changes that are most likely to have an impact on your personal data processing and explained them below. It's not an exhaustive list, but will certainly point you in the right direction.

1. Legal basis for processing

You must ensure that you have a fully legal basis for processing personal data, which is a lot harder to achieve under the GDPR than it was under the DPA. There are now six legal grounds for processing personal data, the two most common for education suppliers being 'legitimate interest' and 'consent'. Processing under either of these grounds is more difficult as consent rules have changed, making it much harder to achieve, and the rules on relying on legitimate interest require you to satisfy several detailed requirements. This is such a substantial area for discussion that we've dedicated a section of this report to it later.

2. Individuals' rights

Your data subjects now have enhanced rights. There are eight which you must be prepared for, and if you haven't already, you'll need to put measures in place to ensure that they enjoy these rights alongside the processing you do.

a) The right to be informed
You need to inform them about your processing of their personal data.

b) The right of access
They must be able to easily access the data you hold on them.

c) The right to rectification
You, or ideally they, must be able to correct or amend the data that you hold.

d) The right to erasure
You must be able to totally destroy that data across all your systems if asked by the data subject.

e) The right to restrict processing
You should have a mechanism in place that allows you to pause/restrict the processing of any data.

f) The right to data portability
You must be able to provide their data to them in a machine readable format.

g) The right to object
You must have a mechanism in place through which a data subject can easily raise their objection to your processing.

h) Rights in relation to automated decision making and profiling
You'll need to ensure that you have suitable measures in place to protect any individual's interests if you employ automated decision making and/or profiling.

3. Accountability and governance

The principles of accountability, governance, and transparency are already requirements of the DPA, but the GDPR elevates their significance. Things you might do to comply are organisationally dependent, but some general ones are the creation of internal data protection policies, staff training, internal audits of processing activities, reviews of internal HR policies, the maintenance of relevant documentation on processing activities, appointing a Data Protection Officer where appropriate, and, if necessary, writing a Data Protection Impact Assessment.

4. Contracts

You'll need to review the contracts you have in place between you and any Data Controllers and Data Processors you have a relationship with. These contracts are mandatory and essential to both your and their understanding of your respective responsibilities and liabilities.

5. Security

This needs to be watertight under GDPR. Data breaches will not be looked at favourably by the ICO, so you'll need to implement measures that ensure against unauthorised or unlawful processing, and against accidental loss, destruction, or damage, of personal data.

6. Fines

Under the GDPR these are a lot greater. Maximum fines for non-compliance under the DPA were £500,000. The GDPR stipulates fines of up to €20 million or 4% of global turnover.

7. Privacy by design

Privacy should be the first thing you think about when designing and implementing new systems. Taking a privacy by design approach is an essential tool in minimising privacy risks and building trust. Designing projects, processes, and products or systems with privacy in mind at the outset can lead to benefits for you and your data subjects.

The legal basis for processing personal data has a higher standard

The GDPR gives six legal grounds for processing data. The two most relevant to you as an education supplier and your marketing are likely to be 'consent' and 'legitimate interest'. You can read about the other four in Article 6.1 of the regulation.

At this point it's worth noting that each of the six grounds are considered equally valid, and choosing one over another will not allow you to comply 'better'. For example, consent is not considered 'more compliant' than legitimate interest, nor is legitimate interest considered 'more complaint' than consent. You need to assess which of them is the most appropriate ground for your different processing activities.

Let's examine both consent and legitimate interest and look at how, under the GDPR, meeting the higher level of compliance for both grounds is going to be more difficult.

Changes to consent

Consent just got a lot harder to rely on. The GDPR, in Article 4(11), has elevated its definition of consent as a legal ground for processing personal data to this:

"Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action signifies agreement to the processing of personal data relating to him or her."

So let's break that down...

"Freely-given" – The data subject must have a genuine choice, and they should not have been misled, or negatively impacted by withholding consent.

"Specific" – It must cover all processing matters, and if more than one processing operation occurs, separate consent is required for each.

"Informed" – You must be clear so that the data subject is aware of who you are and how you intend to process their data. If you've hidden this away in your terms and conditions, or not been explicit at the very point they give you consent, it's not consent.

"Unambiguous" – There should be no room for doubt over the data subject's intentions when providing their agreement that you can use their personal data.

"Statement of clear affirmative action" – There must be a positive indication of agreement by the data subject that is not based on silence, pre-ticked boxes, or inaction.

In Recital 32 of the GDPR it goes on to state:

"Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided."

Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of consent by default.

If you already process a database of data subjects and that list was gained via consent but that consent does not meet these new high standards, then you cannot continue to process that data under the consent ground after 25th May 2018. You'll most likely need to try to re-engage the teachers whose data you hold to opt in to receive your marketing under the consent ground prior to 25th May.

Some of the things we're aware of that go on in our industry that do not qualify as consent under the new rules of the GDPR are:

Getting a School Secretary/Office Manager/member of the Senior Management Team to give consent and update a list of teachers you hold

Getting someone to give consent on behalf of someone else is not consent. It matters not that these teachers are under the employ of a particular school; even if the Head Teacher says it's ok, it isn't. Consent must be freely given and the GDPR is very clear that it must be given by 'he or she' – the individual.

Getting a teacher to sign up for something

Getting a teacher to sign up for something (such as a free prize draw or access to a directory of free teaching resources) and not being 100% upfront about what you're going to do with their data at

point of sign up means you don't have consent. Hiding how you'll process their data away in terms and conditions small print will simply not cut it. It's not consent.

Assuming that a teacher is consenting

Just because a teacher's details are on a school website, or some other online directory, does not mean they have given explicit consent for you to process their data. Remember, for it to be consent, a positive opt-in is required, and it must be explicit.

Allowing teachers to update their data record with a provider online

Simply asking a teacher to 'update their contact details' online, over the phone, or by post, without being very specific about the processing activities you'll perform on that data, is not consent.

Speaking to someone at a school and asking them to verify someone else's data or consent

It might be tempting to pick up the phone, call a school, and ask the person on the line to give you the names and contact information of a bunch of teachers. You can do that if you've ascertained that you have a clear legitimate interest, but doing that does not constitute consent. It must be given by the person themselves (and when you do gain consent over the phone you should also record the phone call* so you're prepared if you're challenged to provide proof at a later date).

* There are laws governing the recording of phone calls so ensure you comply with those before hitting the record button.

Any consent you've gathered for which you do not have a clear and provable audit trail

It's absolutely crucial that you can prove consent in case you are challenged by a data subject or a governing body. The only way to prove consent is with a clear audit trail that shows when, how, and by whom consent was given. Keep copies and screenshots of your consent mechanisms too. If consent was given over the phone you'll need to ensure you have full recordings of each phone call.

Emailing your current list of teachers and saying "If we don't hear from you then we'll assume you've provided consent"

A data subject's silence does not equal consent. Remember, for it to be consent, there must have been a statement of clear affirmative action – not silence or inaction.

Changes to legitimate interest

It's now harder to rely on legitimate interest as a legal ground for processing personal data. This is what the GDPR says about it in Article 6.1(f):

"Processing shall be lawful only if [...] the following applies: [...] Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

And in Recital 47:

"The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest."

There are other things that the GDPR states about the legitimate interest ground, so when considering whether you can rely on it, you need to be aware of four key factors:

1. You'll need to demonstrate that you have balanced your interests with the interests, rights, and freedoms of the individuals affected by your proposed processing activity. This might be very simple or it might be very detailed (when we undertook our consideration at Sprint Education, it was very detailed).

2. You'll need to document it because you may be challenged by individuals or the ICO.

3. You'll need to inform individuals that you are processing their personal information under the grounds of legitimate interest, e.g. via your (GDPR compliant) Privacy Policy.

4. You'll need to honour the individual's right to object to such processing.

Some of the teacher data we process here at Sprint is under the legitimate interest ground. We'd be delighted to share our Legitimate Interest Statement with you; just email guy@sprint-education.co.uk and after you've signed a Non-Disclosure Agreement we'll send you a copy.

Chapter Three:
Sprint Education's GDPR Compliance

Unlike some communication agencies, Sprint is genuinely excited about the GDPR. Its watertight data privacy and security principles, many of which Sprint instituted long before the GDPR was enacted, are, to be frank, long overdue in this increasingly data-driven world. We're also excited at the amazing opportunities and innovation it is driving, not only here at Sprint HQ, but across the digital landscape across the UK, Europe, and beyond.

The GDPR has been on our radar since January 2012, and we started our journey towards compliance way back in June 2014 when the European Parliament first adopted the GDPR. For the next 40 months we scrutinised everything we do with data and it led us to a complete company-wide review of processes, procedures, internal training, data systems, and reviews of policies, documentation, terms, and assessments.

It's been a painstakingly lengthy project in which we have unpicked every word of every article and recital of the regulation consuming eye-watering amounts of time, and energy in the process. We've invested hundreds of man hours and hundreds of thousands of pounds on ensuring that we not only met compliance, but that we transcended it.

We've gone to these great lengths in part so that you and our other clients can rest assured that your education marketing partner is compliant, responsible, and trustworthy. Not only have we achieved compliance but we've also gone above and beyond it (more about that later).

While much of our preparation has happened behind the scenes, some of the work we've done, and are doing, deserves to be shared publicly. We also want to share some of the initiatives we are working on that will further enhance the effectiveness of our clients' communications.

Here's what we've done:

Reviewed Our Legal Basis for Processing Personal Data

In order to ensure that we have a legal basis for processing the 'at work' teacher data we hold and use to broadcast our clients' education communications, we conducted a detailed Legitimate Interest Assessment which identified our legitimate interests for processing data, and examined our processing operations and their purposes, including a necessity test, balancing test, an audit of compensating controls, and our considered conclusions. We finally got this 41-page, 15,614-word document reviewed and approved by a specialist Data Protection and Privacy partner at the UK's leading legal firm on data protection, who act for more FTSE 100 and FTSE 250 companies than any other UK law firm.

If you would like to review a copy of our Legitimate Interest Assessment, please email guy@sprint-education.co.uk to request a copy. You'll need to sign a Non-Disclosure Agreement before the document can be sent to you.

Ensured the Rights of Our Data Subjects

If we cannot ensure the rights of our data subjects, then we're not compliant. So, this is what we've done:

1. Written and distributed a data collection and processing notice

We did this to protect our data subjects' right to be informed.

We've worked through our databases and achieved compliance through the legitimate interest ground. This has included providing every one of our data subjects with a clear and informative Data Collection and Fair Processing notice that identifies our legal ground for processing their data, what we use their data for, how it is processed, and several other things that we are legally obliged to disclose.

2. Created a secure online preference centre

We did this to protect our data subjects' right to have access to – and the right to rectify – their data.

In order to ensure our data subjects have access to the data we hold on them at all times, and to ensure they can update their data at any time if it is inaccurate or incomplete, we've built a non-public-facing, secure, and encryption-led preference centre, where each data subject can review and update their own data and manage their subscription preferences. They can access this via a secure link that is included in the footer of every email we send them. The building of our preference centre has been done in conjunction with some substantial technical adaptions to our databases, and internal software interfaces too.

3. Internal data audit and new terms implemented with clients

We did this to protect our data subjects' right to erasure.

So that our data subjects can have their data erased at a moment's notice, we have undertaken a detailed data audit which has led to all of the personal data we hold now being held in structured and fully-documented places. Furthermore, we have reviewed and updated the contracts we have in place with any third parties to whom we pass out that data.

4. Implemented new database technology

We did this to protect our data subjects' right to restrict processing.

We have implemented technology into our databases which, when activated, ensures that no further processing of a data subject takes place until any restriction is lifted.

Reviewed Accountability, Transparency, Governance

We have audited and analysed all our current services here at Sprint Education, including all facets of our managed email service, our postal service, and Campus, and adapted them to ensure that we, and our clients, are complying with the GDPR when using them. There's more information on this later.

We've also been reviewing contracts with suppliers, planning and delivering internal staff training, implementing an internal Knowledge Base so that all staff are kept fully up to speed with the changes we have made and continue to implement, updated our Data Protection Policy, appointed a Data Protection Officer, and rewritten all privacy policies across all our sites to fully comply with every aspect of the GDPR.

Improved Data Security

We have always held data security at the heart of what we do. We're the only education communications agency to own and fully manage its own servers. To further enhance security of the personal data we hold we have implemented Fail2Ban software on top of our enterprise grade Fortisgate firewall hardware to prevent hackers and attacks.

Our servers now live in four different secure data centres around the UK and Europe to ensure that we have no single point of technical failure and to ensure that we have full-scale backups of all data in different physical locations.

Chapter 4:
Sprint; Above and Beyond Compliance

We don't see being compliant with the GDPR as the ultimate goal. In fact, we've worked hard to ensure that being compliant is our baseline standard. Our clients deserve an education communications agency partner that is using GDPR compliance as the foundation to go above and

beyond, add value, and ultimately offer education communication services that just keep getting better.

We'd like to tell you about some of them.

Gaining Consent from Teachers

"But you've already said that consent is no more compliant than legitimate interest!"

Yes I did, but there's something about consent that really appeals to our transparent values here at Sprint Education. We whole-heartedly believe that by gathering the consent of teachers, we will add value to the data we use to power your communication campaigns. We've also devised an incredible programme which provides teachers that grant consent with amazing perks and benefits for themselves, and their schools. (We will also not withhold access to Teacher Perks if a teacher chooses not to provide consent).

We've implemented some truly exciting mechanisms to obtain consent from teachers, and have already put these into action. Whilst our base legal ground remains legitimate interest for the short to medium term, we've been (and will continue to be) doubling down on our efforts to gain consent. We're targeting a move to work with more consenting teachers in the long-term, and that makes us probably the only agency that already collects opted in teacher consent that complies under the stringent GDPR rules. We don't make that claim lightly either; we've checked up on the consent mechanisms of the other education marketing agencies that claim their data is gained through consent, and whilst some of them have mechanisms that were sufficient before the GDPR, they do not meet the rigours of the new regulations; therefore, they should not be able to use that data under the consent ground since 25th May 2018.

We have made incredible efforts to gain GDPR compliant consent so far, and look forward to this growing and growing over the coming years.

Campus Updates

Our Software Engineers have improved Campus, our Education Sales and Marketing Software, which has included evaluating potential new GDPR-friendly features and templates to add specifically to the software. We have not charged more for these features and we've also added some articles about the GDPR to the Campus Knowledge Base too. We want you to be responsible and compliant!

Launching New GDPR Compliant Services

We launched new services over, plus a whole collection of inbound marketing services designed to help you grow your own list of opt in teachers. Our aim is to be totally 360 degree in our approach to marketing to teachers and schools. We began in 2007 solely as an outreach marketing agency, but have, over the last couple of years, pivoted towards a full marketing approach, now offering outreach, inbound and a discount portal for our clients to advertise discounted products and services to teachers.

Chapter Five:
Sprint's Client-Facing Services

We've worked hard to ensure that all of our services now comply with the GDPR; below is a brief overview of some of them, the poignant changes we've made to them in light of the GDPR, and anything you need to do, or be specifically aware of.

Managed Email Strategies to Teachers at Schools

We've been managing email strategies for education suppliers and organisations from single one-off campaigns to full termly and yearly strategies. These campaigns have always been sent through our own industry-leading sending infrastructure. We're able to ensure that each and every email is very relevant to the recipient through applying dynamic content and personalisation to each campaign. The opens and clicks of the some of the emails we send for clients are recorded so that we can report back to our client about the success of the campaign.

Changes we made

How the email is sent

We changed the way we send emails. We examined how we might shoulder the burden of the Data Controller responsibility for our clients to enable them to continue to get their messages into schools and in front of teachers without the onerous burden of being a Data Controller and having to prove either a legitimate interest or consent ground. So, we now send emails specifically from Sprint Education, and the content is 'sponsored' by our partners. This doesn't change the look of your email much – it is still branded with your livery and written in your specific style, but at the bottom of each email there is a standard footer explaining who we are, a link to one of three preference centres (depending on the data subject in question and the legal grounds under which their data is being processed), and a means to opt out of receiving future messages either from Sprint, or just from ones sponsored by you.

Absolute message relevance

The contents and message of each campaign we send are carefully considered by ensuring that each of the following questions can be answered with, "Yes":

1. Is the communication of particular relevance to the recipient's job role?
2. Is the communication of particular relevance to the establishment type that the recipient works at?
3. Is the communication suitable for the age range that the recipient works with?
4. Does what is being promoted have a clear and specific educational benefit or help the teacher save money for their school, or personally?
5. Is there nothing misleading in the subject line or message?

Unless all five of these can be answered with, "Yes", we won't send the email.

Upscale our sending infrastructure

Although not specifically linked to the GDPR, we've upscaled from 14 to 40+ mail servers, and from 6 to 20+ sending application platforms. This allows us to be more responsible in terms of the number of emails coming from any particular sending IP and spread our sending load across more hardware. This should, in turn, continue to improve our deliverability – and therefore, your response rates.

Changes you need to make

None, we have this covered for you.

Campus Software & Data Subscriptions

Believe it or not, the GDPR was one of the real driving forces behind the creation of our education sales and marketing software, Campus. When we first heard whisperings of the GDPR and its potential impact, we figured that even if it didn't make it into the actual law books (which it obviously did), the landscape of marketing and data privacy would soon change anyway. Campus was designed to assist you in the following areas:

1. Enable you to connect with your target education audience directly by accessing accurate, GDPR compliant education marketing data.
2. Allow you to build good quality relationships with these teachers.
3. Empower you to be able to manage your education business from one place.

Those of you who already use Campus will be aware that there are actually two pools of data in it: The data in the Education Data module which we manage, update, and allow you to use; and your data that you manage and hold in the Contacts module.

This means that we both have responsibilities as Data Controllers under the GDPR.

Education Data Module

For this data, Sprint Education and the client using Campus are joint Data Controllers.

When we process data in the Education Data Module of Campus (like updating it, cleaning it, etc.), we bear the responsibility that it is being processed in line with the GDPR. Similarly, when you process that data (like using it in an outreach marketing campaign), it is your responsibility to ensure that it is being processed in line with the GDPR.

Contacts Module

For this data, the client is the Data Processor and Sprint Education is the Data Controller.

The data held in the Contacts module is your data which you manage and process, meaning that the responsibility of ensuring that it is being processed legally under the GDPR is solely yours. Sprint Education processes this data on your behalf as you require, and so we are the Data Processor; because of this, we have further responsibilities under the GDPR; like being on top of security, and alerting you if there are any data breaches.

How Campus can assist you in your GDPR compliance efforts

Campus already helps you adhere to many of the data subject rights in the following ways:

Right to be forgotten

You can delete individual contacts upon their request at any time. We also built a feature which allows you to create a list of contacts and delete them all at once.

Right to object

All contacts are given the opportunity to opt out by clicking on the unsubscribe link found in the footer of any email. You as a user can also unsubscribe contacts easily from each contact's page in the Contacts module.

Right to rectification

You can access and update your contacts at any time within your Campus account.

Right of portability

You can export your contacts from Campus at any point into CSV format which is a standard format for uploading to other providers.

Help you build your own opt in list of teachers

The Forms Module in Campus allows you to build lead generation forms that you can then easily embed on your website. Then, when a visitor fills them out, their details drop into your Contacts module. This is a great way of generating a list of consenting teachers who you will, providing you have the right privacy notices in place, be able to continue to market to going forward.

Be sure to carefully apply the correct privacy language to the pages on which you host these forms to ensure that it meets GDPR standards. The language should be specific, clear, and cover all the reasons you have for using the information being provided.

Changes we made

To fulfil our obligations as a Data Controller of the Education Data, as your Data Processor, and to help you going forward, we're making some changes:

Publishing a list of organisations that use Campus

As the Data Processor of the Education Data, the GDPR states that we need to inform our data subjects of the third parties who will have access to their data. We are therefore publishing a list of all Campus Partners so that teachers are able to access it through their data preference centre (where they manage their opt in preferences and update their data), so they are always fully informed about who has been given access to their names. This list won't be publically available – it will only be accessible through an encrypted obfuscated link that our data subjects have access to.

Built new features

We built new features into Campus to help you meet your compliance responsibilities. For example you can now access to a Legitimate Interest Assessment template to complete your own assessment with ease.

Changes you need to make

Determine your legal ground for processing your Contacts data

As the Data Controller of the personal data you hold in your Contact Module, you need to ensure that you are abiding by the rules of the GDPR. You'll need to decide on your legal ground for processing.

If you've chosen consent, ensure that all your consent mechanisms meet the higher consent standards. You'll also need to ensure that you're comfortable that the data you've collected and stored in Campus until now meets the stricter consent requirements. If it doesn't, you'll either need to try to re-engage your contacts and gain new 'real consent', or rely on a different legal ground for your processing.

If you've chosen legitimate interest, you'll need to ensure that you've completed your Legitimate Interest Assessment, and inform all your contacts about the legal ground you're using to process their data, as well as their legal rights, and how you came to have their data. You'll also need to conduct a balancing test to ensure that your legitimate interests do not outweigh the rights, freedoms, and interests of them.

Determine your legal ground for processing the Education Data

As the Data Controller of the Education Data you'll need to rely on the legitimate interest ground for processing it legally. This means that you must to be able to demonstrate that you have balanced your interests with the interests, rights, and freedoms of the individuals, inform them that you are processing their data under the legitimate interest ground (you could do that via your privacy policy that you can link to in the footer of the emails you send them), and honour their right to opt out. We'll be providing additional guidance to help our Campus users get this just right soon.

Database of Engaged Recipients

When we run managed email campaigns for clients, sometimes we provide a list of recipients that engaged with the email by downloading the email's images or clicking on any links in it. This gives the client the opportunity to gently follow up these leads.

We are able to pass this data out to named third parties because the teachers are aware we're doing this through the work we've done regarding informing them of our processing activities through the legitimate interest ground. Once this data is passed out to the client, it is then the client who becomes the Data Controller.

Changes we've made

Publishing a list of organisations that access this data

As the original Data Processor of this data, we need to inform the data subjects about the third parties who will have access to their data. So, just like with our Campus users, we are publishing a list of all Engaged Recipient Partners so that teachers are able to access them through their data preference centre (for more information on this, see page 20).

Changes you need to make

Determine your legal ground for processing the Engaged Recipient Data

Just like our Campus users, if you take receipt of Engaged Recipient data, you become a Data Controller and so, as above, you'll need to rely on the legitimate interest ground for processing it legally. See the answer to 'Determine your ground for legal processing for the Education Data ' on page 20 which explains this.

Postal marketing

We send postal communications to teachers at schools and sometimes address the mail piece with the teacher's name.

Changes we've made

We've already proven a legitimate interest to process teacher data in this way and so no further changes are necessary.

Changes you need to make

None, we have this covered for you.

Chapter Six:
Questions to Ask Your Marketing Partner

If you currently do not use Sprint Education as your education marketing partner, I strongly urge you to contact the agency you do work with (or are considering working with), and ask them questions about how they comply with the GDPR. They should be able to talk confidently about it; how it affects their services, what you should ensure you're doing to comply, their legal ground for processing personal data, and the work they've done that surrounds them relying on it.

Under the GDPR, choosing your education marketing partner becomes even more important. You don't just want a partner who is great at marketing to schools and teachers, but also one who you know has taken the GDPR seriously and used it as a force to instigate positive organisational change that will ultimately benefit you.

We've put together some questions that you should use to form a deeper conversation with your education marketing partner. Have the conversation sooner rather than later, use the questions below, and you'll soon get a feel for how responsible they are.

How do you ensure that the teachers' numerous rights under the GDPR are respected?

If your marketing partner is emailing teachers at schools on your behalf, providing you with any personal data for your own marketing, or using their database to run a postal campaign for you then they will, under the GDPR, be a Data Controller which comes with significant legal responsibilities.

They should be able to tell you what internal measures they have put into place to ensure the numerous rights that data subjects have, and be able to demonstrate to you what internal measures they're putting in place (or already have in place) to ensure right of access, right to rectification, right to erasure, right to restriction of processing, right to data portability, and right to object.

Sprint's answer: *Read all about what we've done to protect teachers' rights on pages 14 and 15.*

Under what legal ground do you process teachers' 'at work' data?

Your partner will likely be processing teacher 'at work' data either under legitimate interest, under consent, or (worst case scenario) not legally at all. They should be able to talk confidently to you about what legal ground they have chosen and why, as well as the internal work they've needed to do to ensure that the ground they have chosen is appropriate. You might extend your question to: "Why have you chosen this legal ground over the over five that are available?"

Sprint's answer: *We process some personal teacher 'at work' data under the legitimate interest ground, and some under the consent ground. You can read more about that on pages 14 – 16.*

Can I see a list of your online consent mechanisms?

(Ask this if they are using consent as their legal basis for processing).

A consent mechanism is the vehicle through which a data subject gives consent (usually a form on a web page). If your partner is using the consent ground then they should be able to give you a list of web pages where these data capture points exist. Be sure to scrutinise these consent mechanisms to satisfy that if the teacher fills out the form they are actually giving consent under GDPR – remember, consent is:

"Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action signifies agreement to the processing of personal data relating to him or her."

There should be no pre-ticked checkboxes, and the explanation of how and why they'll process that data going forward should not be hidden away in terms and conditions legalese. It must be very upfront and honest, and there should be zero room for doubt over the data subjects' interpretation of what they are giving consent to.

Sprint's answer: *Take a look at our main consent mechanism on our Teacher Perks site here: www.teacherperks.co.uk.*

Can you provide an audit trail of when and how consent was granted?

(Ask this if they are using consent as their legal basis for processing).

Consent is only consent if you can prove it, otherwise it's worth nothing. Your marketing partner should be able to tell you when, and by what means, each of their data subjects consented. This should include them being able to provide you with a URL or screenshot of the consent mechanism through which consent was given.

Sprint's answer: *We can provide you with this information for every individual whose personal data we process under the consent ground.*

Can I see your Legitimate Interest Assessment, including your balancing test?

(Ask this if they are using legitimate interest as their legal basis for processing).

If your marketing partner is using legitimate interest as the ground for processing the data then they will have needed to document a Legitimate Interest Assessment which identifies their legitimate interest, that it is appropriate, the processing operation and its purposes, a necessity test, an examination into alternative grounds, a balancing test, and an analysis of safeguards and compensatory controls, as well as their documented outcomes. If they cannot provide you with this (expect to have to sign a Non-Disclosure Agreement before it's passed to you) then they've not done their due diligence, and it's possible that they are not processing personal data legally.

Sprint's answer: *We'd be delighted to share our Legitimate Interest Assessment with you. Simply get in touch and after you've signed a Non-Disclosure Agreement we'll email you a copy.*

Can you provide me with an audit trail of when and how you informed the data subject about how you got their data, how you process it, under what legal ground it is processed, and their right to object?

(Ask this if they are using legitimate interest as their legal basis for processing).

If your marketing partner is processing personal data under the legitimate interest ground, then it's recommended that they've provided each data subject with clear and informative information about how they got hold of their data, what they specifically do with it, and that the subject has fundamental rights under the GDPR (they actually need to be clearly reminded of those rights by the controller). If your partner cannot provide you with this information, it could also follow that they have not provided this information to each and every data subject.

Sprint's answer: *We can provide you with this information for every individual whose personal data we process under the legitimate interest ground.*

You're passing out teacher data to me as a third party. Have you informed every teacher that I have that data?

If your marketing partner is providing you with personal data to use yourself – whether that's as a spreadsheet, CSV, or access via an online portal – then they, as the controller of that data, must have informed every data subject that they are doing that. Ask them how they do that, and how each data subject can object to that part of the processing.

Sprint's answer: *We have informed every teacher whose personal data we process through a Data Collection and Fair Processing Notice. You can read about that on page 14.*

How have you informed your data subjects that you track their email opens and clicks?

If your marketing partner is managing an email campaign for you and sending that campaign to their own list of teachers, then it's likely that they've also told you they'll track the email and provide you with a report of opens and click-throughs. It is important that the data subjects are aware that this tracking is going on, so you should ask your partner by what means they have informed each and every data subject prior to your campaign being sent.

Sprint's answer: *We have informed every teacher that we may track the opens and clicks on the emails they receive from us in the Data Collection and Fair Processing Notice we provide them with. You can read about that on page 14.*

Can I see a copy of your Data Protection Policy?

Any organisation worth their salt has a Data Protection Policy. If your marketing partner cannot or will not provide you with a copy of this (or any other internal policy), how can you be sure that they are being responsible?

Sprint's answer: *Yes certainly. You can see that in the Legal section of our website.*

Chapter Seven:
Leasing Personal Data

Occasionally I'll speak to an education company that has been informed by another education agency that under the GDPR they are not permitted to lease their teacher email data, and that the only option is to pay for generic (office@... type email) data.

I could hypothesis why an education agency or data provider might inform education companies that this is the rule. Is it the data as accurate as they claim? Do they have the number of records that they claim? Have even read GDPR regulation at all?

To clear this up, it's best to go directly to the UK's data regulators and see what they have to say. Here is the ICO's published position on passing out personal data without consent.

The ICO's 'Direct Marketing Detailed Guidance'

The ICO state, in their 2022 'Direct Marketing Detailed Guidance' (published 5th December 2022) that a data broker may rely on legitimate interest to share personal information as long as they comply with data protection law and PECR.

(Source ICO: https://ico.org.uk/for-organisations/direct-marketing-guidance-and-resources/direct-marketing-guidance/plan-direct-marketing/#canweshare)

They give specific examples of the requirements:

1. Tell people you want to share their information.
You must make clear to people that you want to share their information with other organisations for direct marketing purposes.

Sprint does this in the data collection and fair processing notice provided to all data subjects before their personal data is actively processed. It is also provided in the privacy policy available to our data subjects in their own personal preference centre.

2. Be able to justify sharing using legitimate interests.

If you want to use legitimate interests as your data protection lawful basis, you must look at whether people would reasonably expect you to share their information with others for direct marketing.

Sprint informs the data subject before any active processing takes place via the data collection and fair processing notice so it is reasonable to expect that they expect we will do what we state.

3. Give people a chance to opt out of the sharing.

If you are not relying on consent, then as a safeguard when you first collect information from people, you should include a clear, simple opt-out opportunity. People can use this if they want to object to you sharing their details with other organisations for direct marketing.

In the data collection and fair processing notice data subjects can click through to their personal preference centre where they can opt out of us sharing their data.

4. Take PECR into account.

If you want to share a marketing list for other organisations to use to send electronic marketing messages, you must take PECR into account.

Sprint does take PECR into account. Teachers and School Staff are considered corporate subscribers and under PECR these data subjects may be emailed with direct marketing without consent as long as a legal basis for processing under GDPR (legitimate interest) is held.

Furthermore, on the ICO's website 'for organisations' section, they answer the following:

Can we use legitimate interests to disclose data to third parties?

You may be able to lawfully disclose data on the basis of legitimate interests. These might be your own interests, or the interests of the third party receiving the data, or a combination of the two.

Your focus is on justifying your disclosure when you carry out the three-part test. Although the third party's intentions and interests are directly relevant, your focus is on whether the disclosure itself is justified for that purpose. The third party is responsible for ensuring their own further processing is fair and lawful, including carrying out their own three-part test if they plan to rely on legitimate interests as their basis for processing.

Source ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/#third_parties

Client Becomes Data Controller

When teacher/school staff personal information is passed out to the third party they become the data controller of that data. This is because they exercise overall control over the purposes and means of the processing of personal data going forward.

The ICO states:

The third party is responsible for ensuring their own further processing is fair and lawful, including carrying out their own three-part test if they plan to rely on legitimate interests as their basis for processing.

Source ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/#third_parties

Glossary

Here are some commonly used terms that relate to the GDPR and marketing to teachers at schools:

Consent

Freely given, specific, informed, and explicit consent by statement or action signifying agreement by the data subject to the processing of their personal data by the Data Controller.

Corporate Subscriber

Companies, other corporate bodies (e.g. limited liability partnerships), Scottish partnerships, and government bodies (e.g. state schools).

Data Controller

The organisation that determines the purposes, conditions, and means of the processing of personal data.

Data Erasure

This is also known as the Right to be Forgotten and gives data subjects the power to demand that their personal data is erased by the Data Controller.

Data Portability

This is a requirement for Data Controllers to provide any data subject with a copy of their data in a format that allows for easy use with another controller. It should usually be provided in easily machine readable format (e.g. a CSV file).

Data Processor

The organisation that processes data on behalf of the Data Controller. For example your CRM provider would be your Data Processor.

Data Protection Act

The Data Protection Act 1998 is a UK Act of Parliament designed to protect personal data stored on computers or in an organised paper filing system. It follows the EU Data Protection Directive 1995.

Data Protection Authority

National authorities that ensure the protection of data and privacy as well as enforcing and monitoring data protection regulations. The UK's DPA is the Information Commissioner's Office (also known as the ICO).

Data Protection Officer

An expert on data privacy. They provide independent guidance and ensure that an organisation is following the rules of the GDPR.

Data Subject

A natural person whose personal data is processed by a controller or processor.

Direct Marketing

The communication of any advertising or marketing material which is directed to particular individuals, by whatever means.

Directive

A legislative act that sets out a goal that all EU countries must achieve through their own national laws. An example of a directive is the ePrivacy Directive that forms the basis of the UK's PECR.

Encrypted Data

Any data that is protected through technological measures so that it is only accessible/readable by those with specified access. Encrypted data is often called 'obfuscated' because it looks like unintelligible strings of characters.

ICO

The Information Commissioner's Office. They are the UK's Data Protection Authority and are tasked with ensuring that we all abide by the requirements of the GDPR.

Personal Data

Any information related to a natural person or 'data subject' that can be used to directly or indirectly identify the person. Examples are, amongst others, name, email address, physical address, biometric data, and financial data.

Privacy by Design

A principle that calls for organisations and individuals to think about the inclusion of data protection at the outset of designing systems, rather than as an afterthought.

Privacy Impact Assessment

A tool used to identify and reduce the privacy risks of organisations by analysing the personal data that is processed, and the policies in place to protect this data.

Processing

Any action performed on personal data, whether or not by automated means. This includes collection, storage, editing, usage, etc.

Profiling

Any automated processing of personal data to enable you to evaluate, analyse, or predict a data subject's behaviour. If you are profiling, there are even more stringent requirements to adhere to under the GDPR.

Pseudonymisation

The separation of data from direct identifiers so that linkage to an identity is not possible without additional information that is held separately. It's used to reduce risks associated with data processing – especially when the data processing involves special/sensitive categories, like health records.

Regulation

A binding legislative act by the EU that must be applied in its entirety across the Union. It's basically a 'step up' from a directive.

Right to Access

This principle entitles the data subject to have access to the personal data that a controller has concerning them.

User

A person who works for a corporate subscriber and who uses their communication infrastructure in their daily work.

Further Reading

The full text of the GDPR

http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

The Information Commissioner's Draft Guidance on Direct Marketing

https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf

The Information Commissioner's Draft Guidance on Consent

https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf