Data Protect Policy

Date: 25th June 2018

This policy defines PEAS approach to ensuring the protection of personal information processed by PEAS, with a focus on complying with the European Union's General Data Protection Regulation ("**GDPR**"), which comes into force on 25th May 2018.

Table of Contents

1 The General Data Protection Regulation ("GDPR")

1.1 Introduction to GDPR

The General Data Protection Regulation (**"GDPR"**) is an EU Regulation, which comes into effect from **25th May 2018**. The GDPR is designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens data privacy and reshape the way organisations approach data privacy.

GDPR applies to all organisations **operating within the EU**, including corporates, charities and public bodies. It applies to any processing of personal information of a data subject who is an **EU citizen** – where:

- **'processing'** is defined as any operations performed on personal data, whether or not by automated means, such as collection, recording, storage and retrieval.
- **'personal information'** is defined as any information relating to an identifiable, living person who can be directly or indirectly identified by it. This includes a person's contact details, date of birth and their IP address.
- A **'data subject'** is defined as the individual who is the subject of the personal data, i.e. the individual about whom the personal data is about.

In the UK, GDPR is regulated by the **Information Commissioner's Office ("ICO")** – an independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Under GDPR, the maximum fine is **up to €10,000,000** (or 4% global turnover) for negligence and non-compliance.

To ensure PEAS is GDPR compliant, we must ensure all processing of personal information by PEAS considers **data protection by design**, is **fair** and is **in line with the expectations of the individual**. PEAS' processes for collecting, storing and using data must ensure we only hold the data we genuinely need for each specific purpose, use it appropriately, and ensure it is secure. If an individual does not understand what we are doing with their personal data – then we cannot do it, whatever it is.

1.2 Conditions for processing data

As specified in Article 6 of the GDPR, there are six available lawful bases for the processing of personal data. One of these condition must be satisfied in order to process personal data. The three most relevant to PEAS are:

- **Consent** – any freely given, specific, informed and unambiguous indication in which the data subject agrees to their personal data being processed. Consent cannot be assumed when processing data - failure to opt-out is not consent, silence is not consent, making a donation is not consent, previous support is not consent. Consent must be requested in clear and plain language.

  In PEAS' case, we rely on collecting consent for adding individuals to our mailing list. When an individual is added to our list, they provide their communications preferences for being updated on our work, the latest on our impact and opportunities to support our work.

  Another example would be when an individual signs-up to attend an event organised by PEAS, they provide consent to their information being processed in relation to that event. This does

not mean that PEAS will add them to our mailing list – that individual most provide their explicit consent for any processing that is not in relation to the event.

- **Legitimate interests** – the processing of data is necessary for a legitimate interest – this can be in PEAS' interest, the data subject's interest or the interest of third parties and beneficiaries – which is a very broad definition for a charity. Two considerations are important:

  1. Is the processing necessary for that purpose? If there is another reasonable and less intrusive way to achieve the same result, you cannot rely on legitimate interests.
  2. Do the data subject's interests override the legitimate interest? You must balance your interest against the rights and freedoms of the data subject. If they would not reasonably expect you to use their data in that way, or it would cause them unwarranted harm, their interests likely override yours.

  In PEAS' case, we rely on legitimate interest for:

  - Researching a potential partner or donor. In this case we only process information which is relevant for this purpose and does not infringe on the rights and freedom of the individual, combining information which is publicly available with our own information. This will ensure that any future communication is tailored to the individual.
  - Reaching out to a new or existing contact. When reaching out to an individual, for example a cold outreach to a potential funder or an individual from a peer organisation, PEAS will rely on legitimate for this contact. If the individual asks not to be contacted again, to have their information deleted or asks where we found their contact information – PEAS must oblige.

- **Necessary to fulfil a contract** – the processing of data is necessary in relation to a contract which the data subject has entered into, or because the data subject has asked for something to be done so that they can enter into a contract.

  In PEAS' case, we may need to process personal data in order to administer a grant agreement, donation or employment contract.

The three other legal bases – legal obligation, necessary to protect vital interests and legal power / public function, are deemed to not be relevant to PEAS at the current time.

In the case of processing **sensitive data categories** (i.e. racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual life, criminal proceedings), there are additional conditions that are defined in GDPR. However, as PEAS does not process this information except where it is required to fulfil employment obligations, this has been omitted from this Policy.

2 PEAS Approach to GDPR

This section describes how PEAS have approach GDPR as an organisation, and how we have looked to implement data protection by design – reshaping our processes and policies to consider data protection at its core, rather than reactively considering it as a last step. As a team, PEAS has approached this topic with as much thoroughness as can be reasonably expected from an organisation the size and scale of PEAS. However, we are always open to learning from others and re-shaping out approach, and will continue our conversations with peer organisations, partners from other industries and trustees to evolve our approach.

PEAS conducted an analysis of existing policies and procedures to identify five core streams of activities:

1. Collection of personal information
2. Storage of personal information
3. Data Breaches
4. Training
5. Governance

2.1 Collection of personal information

This refers to how we collect personal information and keep it up-to-date.

2.1.1 Consent

As described in Section 1.2, PEAS gathers consent for our 'mailing list' – i.e. the processing of personal information for individuals who want to keep updated on our work, the latest on our impact and opportunities to support our work. The main means of being added onto this list and providing consent is via our sign-up form hosted on Mailchimp, however PEAS can also collect consent via email or speaking to someone on the phone or face-to-face (see Appendix A: Phone script for gathering consent (for PEAS staff answering phone) for the phone script for gathering consent). The key features for gathering consent are:

- **Transparency** about what information we process, how we process it and for what purposes.
- **Never assuming consent** – we must obtain a positive 'opt-in' for all future communications.
- Ensuring individuals are **aware of their rights** to withdraw or update their information, or ask for their information to be forgotten – and how they enact these rights.

In order to demonstrate that PEAS has collected consent, we must maintain a record of what consent was collected and how the consent was collected:

- **For those who maintain their information online** – consent is recorded via the Mailchimp sign-up form. These contact details are then updated on Salesforce on a regular basis (new contacts are added, existing contacts are updated).
- **For those who maintain their information via phone or personal contact** – after collecting consent via phone or personal contact, an email must be sent to the individual declaring the consent that was collected. This contact is then saved onto Salesforce – and the email and any other proof of consent is attached to the contact.

PEAS will continue to process personal information without consent where the GDPR legislation allows us to do see, as specified in Section 1.2.

2.1.2 Automated Profiling

GDPR implements strict controls on 'profiling' – the use of automated techniques to evaluate certain aspects of an individual, in particular to predict an individual's economic situation, personal preferences, interests, behaviour or movements. In particular, this refers to using computer-based analysis for decision-making – researching an individual to create a profile of their interests isn't enough to fulfil this criteria, this profiling must be done using a computer programme or automated processing.

At present, PEAS does not use a computer-based analysis for profiling, and therefore these controls do not apply.

2.2 Storage of personal information

2.2.1 List of contacts

PEAS will have one golden list of contacts, stored securely on Salesforce along with a record of any consent collected. As other platforms may be used to initially collect information will also store personal information, such as Mailchimp and our Raising IT website, however these will be used to update the golden list stored on Salesforce.

PEAS may need to write other improvised lists of contacts, for example when organising an event, when preparing to attend a conference or when reviewing candidates for a PEAS role. When this happens, PEAS will store the information in a secure folder on Dropbox or Google Drive, with restricted access and with clear guidance that the file should not be downloaded and stored on the hard drive of any device. Only information that is required for the purpose should be included, and the information should be deleted once it is no longer required.

All other lists of personal information that existed before GDPR were deleted

Ahead of 25th May 2018, the PEAS UK team undertook an exercise to go through Dropbox, Drive and Gmail files to delete any personal information which is not GDPR compliant, with as much thoroughness as can be reasonably expected from an organisation the size and scale of PEAS.

2.2.2 Sharing Personal Information

Only selected PEAS UK staff will have access to personal information. Under any circumstances where personal information needs to be shared with PEAS Uganda or PEAS Zambia staff, for example ahead of a visit to a PEAS school, consent from the individual will be sought.

As specified in PEAS Employee Privacy Statement, there may be cases where personal information of prospective or current employees or volunteers is shared with the PEAS Uganda or PEAS Zambia teams.

PEAS will not sell or swap personal information with any other organisation. PEAS may disclose personal information if required to do so by law or if we believe that such action is lawful and necessary to protect and defend the rights, property or personal safety of PEAS and our stakeholders and for other lawful purposes.

PEAS may share personal information with trusted partners, agents or service providers to help us with our work.

2.2.3 Service Providers

As part of the initial project to implement and comply with GDPR, PEAS reviewed the service providers with which personal information is shared. PEAS will only share personal information with third-party service providers who take GDPR and data security seriously. PEAS consolidated the platforms utilised to process data to the following 'data processors' listed in **Appendix C**.

2.3 Data Breaches

GDPR introduces a duty on all organisations to report certain types of personal data breach within 72 hours of becoming aware of the breach. A personal data breach refers to any security incident which affects the confidentiality, integrity or availability of personal data held by PEAS.

PEAS takes full responsibility for all the data it processes, so whether a breach occurs due to unavoidable theft, actions of a PEAS staff member or of a third party service provider, PEAS will respond. PEAS considers it important to have controls and training in place to avoid breaches, mechanisms in place to detect breaches and processes for reporting breaches that do occur.

2.3.1 Avoiding breaches

In many ways, all the processes and policies refer to in this policy are part of avoiding personal data breaches. By considering data protection by design, PEAS seeks to minimise the risk of breaches of personal information.

PEAS also recognises that establishing strong processes and policies come to nothing if the PEAS staff who process personal information are not trained and familiar with them. As such, PEAS considers the training of PEAS employees and volunteers described in Section 2.4 as a key component to avoiding breaches.

2.3.2 Detecting breaches

One of the key mechanisms for detecting breaches is for PEAS staff and volunteers to recognise when a breach has occurred, and to report it to the PEAS COO (responsible for data protection in Section 2.5) without delay for further investigation. PEAS has conducted training on recognising and reporting data breaches through the PEAS Data Breach Record form, and by being clear that any failure to comply may result in dismissal.

Through the service providers selected by PEAS, there are also centralised mechanisms by which PEAS may become aware of a breach, for example if an unfamiliar device attempts to access Google Drive or if a large volume of content is deleted from Dropbox. In these cases, the PEAS COO will be notified without delay for further investigation.

2.3.3 Reporting breaches

PEAS has the following Data Breach Process once a breach has been detected and reported to the PEAS COO:

1. **Report the breach** on the PEAS Data Breach Record, which notifies PEAS COO of the breach.
2. **Take immediate measures to minimise impact**, for example the remote wipe of devices or restricting access to files. PEAS COO is responsible for coordinating the response to the breach.
3. **If the breach is material, immediately notify the Global Strategy Team (GST)**, to conduct an assessment of the breach to identify the scope of the breach, the risk likelihood and severity and any measures to mitigate any possible adverse effects.

4. **Depending on the risk, notify the ICO & the Board.** If the breach is likely to result in a risk to people's rights and freedoms, then the ICO must be notified within 72 hours of becoming aware of the breach and the PEAS Board of Trustees will be notified[1] simultaneously.
5. **Depending on the risk, notify the individual.** If the breach is likely to result in a *high* risk to the individual's rights and freedoms, then the individual concerned must be notified as soon as possible.
6. **Investigate the breach**, identifying any measures that should be taken to mitigate the impact and minimise the risk of the breach reoccurring. All breaches **must be documented** – even if they were not deemed to warrant a notification at step 3 and 4.

2.4 Training

PEAS recognises that training PEAS employees and volunteers will be key to ensuring PEAS adherence to GDPR. Employees must be aware of both the risks to the organisation, as well as the risk to themselves. All PEAS UK employees will be trained that any failure to comply with this Data Protection Policy may result in dismissal.

PEAS has developed three training approaches:

- **Launching GDPR (around 25th May 2018)** – for PEAS UK staff, Country Directors and grant managers.
- **GDPR induction training** – for all relevant employees and volunteers joining PEAS.
- **Refresh training** – every two years, to all relevant employees and volunteers.

Topics to be included in this training range from GDPR-specific topics, to general best practice with regards to data protection and IT security:

- Introduction to GDPR
- PEAS responsibility under GDPR
- What is personal information?
- Storage of personal information
- What is a data breach?
- What to do in the event of a data breach
- General IT security principles
- Best practice for IT security

PEAS will always be open to ideas from peer organisations, partners from other industries and our trustees on mechanisms for embedding data protection in the organisation.

2.5 Governance

2.5.1 Responsibility for data protection

As part of the legal responsibilities of a Board of Trustees, the Board is ultimately responsible for data protection and the implementation of GDPR. PEAS will have at least one designated trustee to oversee the implementation of GDPR and data protection practices within the organisation.

In practice, PEAS COO has overall responsibility for data protection on PEAS' Global Steering Committee, working closely with the HR and Business Development teams on implementation.

[1] The Communications Policy will also be attached, which outlines PEAS' Crisis Response Plan.

2.5.1.1 PEAS does not have a Data Protection Officer

Under GDPR, an organisation must appoint a Data Protection Officer (DPO) if they are a public authority, if their core activities require large scale, regular and systematic monitoring of individuals or if they conduct large scale processing of special categories of data. PEAS does not fulfil any of these criteria.

An organisation can still appoint a DPO, even if they are not required to do so. This DPO would be responsible for advising the organisation around data protection, monitoring compliance with GDPR and be the first point of contact for supervisory authorities or individuals whose data is processed. However, the DPO cannot hold a simultaneous position within the organisation which could lead to a conflict in interests, for example they cannot determine the purpose of any processing of personal information.

Due to its size and scale, PEAS does not have a dedicated IT Security or Compliance function. As such, PEAS is **not appointing a DPO** – and instead the responsibility around the implementation of policies, monitoring of compliance with GDPR and coordinating responses to supervisory authorities or individuals whose data is processed is held by PEAS COO.

2.5.2 PEAS employees' responsibilities for data protection

This policy applies to all employees, workers, volunteers, contractors, consultants, directors and any others who process personal data on behalf of the organisation. You must read, understand and comply with this policy when processing personal data on PEAS' behalf and attend training on its requirements.

However, all PEAS employees are responsible for ensuring compliance with this policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

Failure to comply with this policy will be regarded as serious misconduct and will be dealt with in accordance with the organisation's disciplinary procedure.

2.5.3 Monitoring and Reporting

Data protection will be monitored and reported through PEAS' Risk Management Process as a risk on the Risk Inventory. As specified in Section 2.3.3, any breaches of personal information will be reported and recorded in line with the Data Breach Process.

2.5.4 Key documentation

PEAS has put in place and collected a range of documentation to ensure compliance with GDPR. PEAS' approach to data protection and GDPR, and all associated documentation, will be reviewed at least **every two years** to ensure PEAS continues to comply with relevant regulations and ensures protection of its data with as much thoroughness as can be reasonably expected.

The key documentation can be summarised as followed:

2.5.4.1 Data Protection Policy

This policy details PEAS' approach to ensuring the protection of personal information held by PEAS, with a focus on the implementation of GDPR. It explains how PEAS has considered and implemented various components of relevant data protection regulations, and is designed to be the main document in which we evidence our thought process around data protection.

This document is reviewed by and owned by the Board of Trustees.

2.5.4.2 PEAS' Privacy Statement

PEAS' Privacy Statement lives on the PEAS website and has been written to ensure that all data subjects understand how their data will be processed by PEAS, as they have a right to understand what we are doing with their personal information. PEAS' supporters are directed towards this statement via any means of collecting consent, therefore this is a key document for ensuring PEAS' compliance with GDPR.

This document is owned by PEAS and may be edited and enhanced, based on feedback from our data subjects and other partners. All versions of the document must be stored.

2.5.4.3 PEAS Employee Privacy Statement

PEAS Employee Privacy Statement is a key document provided to all PEAS UK employees and volunteers during the recruitment and induction process.

As with the PEAS Privacy Statement, the Employee Privacy Statement has been written with language designed to be transparent and understood by all readers, with no attempt to hide or exclude any details which may be of interest to the data subjects. PEAS has drafted this by reviewing relevant regulations, looking at peer organisations and asking consultancies for their advice.

2.5.4.4 PEAS Candidate Privacy Notice

PEAS Candidate Privacy Notice will be posted publicly on the PEAS website and shared throughout the recruitment process. The notice has been written to inform all candidates about how PEAS processes their personal data during the recruitment process.

As with the PEAS Privacy Statement and Employee Privacy Statement, the PEAS Candidate Privacy Notice has been written with language designed to be transparent and understood by all readers, with no attempt to hide or exclude any details which may be of interest to the data subjects. PEAS has drafted this by reviewing relevant regulations, looking at peer organisations and asking consultancies for their advice.

2.5.4.5 PEAS Data Breach Record

PEAS has designed a Google Form for employees to record any data breach detected, which in turn alerts the COO. The Data Breach Reporting process will then be followed accordingly. Regardless of whether the GST, ICO, Board or individuals are informed, PEAS will maintain this Data Breach Record of all data breaches recorded.

2.5.4.6 Employment Contracts

Employment contracts for existing employees will not be amended but they will be issued with the employee privacy statement. All new employment contracts and volunteer agreements will include a GDPR compliant clause.

2.5.4.7 Evidence

PEAS must record measures taken to comply with the GDPR, in order to demonstrate that we are compliant. These will be stored in the **GDPR Evidence** Dropbox folder.

The types of records which could be included are:

- Trustee meeting minutes when Data Protection has been discussed;
- Policies, procedures and employee guidance relating to Data Protection;
- All versions of PEAS' Privacy Statement, which is hosted on PEAS' website;
- Records of staff induction and training – who, what and when;
- Records of any monitoring, audits or reviews aimed at checking that policies and procedures are fit for purpose and being followed; and
- Records of incidents or breaches, how they were handled and what was learned.

Appendix A: Phone script for gathering consent (for PEAS staff answering phone)

If someone rings the PEAS phone number and wants to sign-up to hear more information about PEAS, you must run through the following script in blue.

"As you may know, organisations in the UK are subject to new data protection laws, which include ensuring that you are aware of both your rights and how we, as a charity, use your data. I can provide with this information just now over the phone and then record your consent, which will take 3-4 minutes – or if you prefer, I can email you a link to our sign-up form and the full Privacy Statement, which may be more convenient for you.

Would you like to hear this information and provide consent on the phone, or would you prefer to receive the information and sign-up via email?"

If their preference is via the telephone, you must talk through the following script:

1. Your personal information that we are discussing today will be stored and used by the UK charity PEAS – which stands for 'Promoting Equality in African Schools'. You can contact us on +44 (0)203 096 7700 between 9am and 5pm, Monday to Friday. You can also email us at info@peas.org.uk, visit our website at www.peas.org.uk or send us a letter at 7-14 Great Dover Street, London SE1 4YR.

2. For any enquiries specifically regarding data we store about you, or how PEAS uses your data, you can contact our Chief Operations Officer at dataprotection@peas.org.uk or write to them at our company address marking your letter for the attention of the Chief Operations Officer.

3. We collect information purely for the purpose of helping our work towards our mission. Specifically, PEAS processes information in order to administer donations and enquiries, to contact people if we need to, to help make our website better, to understand why people support our work, to carry out due diligence on our donors and – should you agree that we may do so – to keep you updated on our work and our impact, and to share future opportunities to support our work.

4. We will always keep your details safe and will not sell or swap your information with any other organisation. We may share your information with trusted partners, agents or service providers, and have contracts in place with our suppliers requiring them to comply with the UK's law on data protection.

5. We will hold your personal information on our systems for as long as it is lawful and necessary to do so. You have right to access, update or erase the personal information we hold, or to request that we stop using your information at any time – to do this, just email dataprotection@peas.org.uk or phone us.

6. Our full Privacy Statement, which contains further details on all aspects of PEAS' approach to Data Protection, can be found on our website: www.peas.org.uk/privacy. We are also happy to answer any questions you have, just email dataprotection@peas.org.uk.

7. Given everything that has been stated, please can you provide me the following information (note – not all fields are mandatory):

    a. Name (First Name and Last Name) - *mandatory*

    b. Email address – *mandatory*

    c. Organisation Name (if applicable) – *not mandatory*

    d. Address: - *not mandatory*

i. Street Address

ii. City

iii. Post Code

iv. Country

e. Phone Number: - *not mandatory*

f. We would like to keep you up-to-date with our progress, our impact and future opportunities to support us: - *mandatory*

i. Are you providing your consent to receive this information by email? Yes / No

ii. Are you providing your consent to receive this information by telephone? Yes / No

iii. Are you providing your consent to receive this information by post? Yes / No

iv. Are you providing your consent to receive this information by text message (SMS)? Yes / No

8. In order to comply with UK data protection law, we will be sending you an email to the email address you have provided clarifying everything you have provided consent for today.

9. As we mentioned earlier, you have the right to withdraw or update consent, lodge a complaint with a supervisory authority, or request that all personal information held by PEAS is deleted at any time. To do this, please email dataprotection@peas.org.uk or call us on +44 (0)203 096 7702.

10. Do you have any questions at this time?

11. Thank you very much for your ongoing support. Have a lovely day.

Take all the information collected in (7) and send in an email to dataprotection@peas.org.uk, who will update our contact list and send an email to the caller. This email must be uploaded as evidence of consent.

Appendix B: Phone script for dealing with individuals exercising their rights (for PEAS staff answering phone)

The following is guidance for all PEAS employees, volunteers and workers to use when an individual calls PEAS to exercise their rights under GDPR. A script has been created to ensure you are dealing with their request correctly and to collect all the information necessary. The script is highlighted in **blue**.

Step one: Collecting basic information

In order to ensure we address your request appropriately, I will need to collect some basic information from you today – and one of my colleagues who manages our data protection procedure will follow up with your request within 3 working days.

All the information I collect from you on this call will only be used for the purpose of dealing with your request; once your request has been dealt with appropriately, we will delete all the information collected.

In line with the requirements of GDPR, all requests will be responded to within one calendar month – however, we aim to address the request as soon as possible.

May I ask for your

- First Name and surname
- Phone number
- E-mail address

Would you prefer my colleague to contact you in regards to your request by telephone or e-mail?

Step two: Reason for calling

What is your reason for calling today? What would you like us to do with your personal information?

Their response should relate to one of the following rights, however, note they may want to exercise more than one of their rights such as right to be informed and right of access. Identify what right it is and ask the corresponding questions or advise the information highlighted in blue.

1. **Right to be informed / Subject Access Request– they would like to see what data PEAS holds on them**
    - What type of information do you want to see, in particular?
      Note: They don't have to specify, they can just say all information, however it would be preferable to get some context on the request.
2. **Right of access – they would like to know what personal information PEAS is processing and how**
    - How would you like to receive this information? (Phone, email or post. If post, ask for their address).
3. **Right to rectification – they would like to add or change the information that PEAS holds on them**
    - What piece of information would you like to update?
    - What would you like to update it to? We will either call for more information, or email confirming this has been done
4. **Right to be forgotten – they may want PEAS to delete all information on them**
    - We will email you when we are about to delete all your information, so you know it has been done. We will then delete that email, so we have no more of your personal information.
5. **Right to restrict processing – they would like to restrict or change the way that PEAS is processing their data**

- Can you provide some additional context? What type of processing would you like to change? My colleague will contact you to ask for more information, or confirm this has been done.

6. **Right to portability – they would like to get a copy and reuse their own personal information for their own purpose**
    - Do you know what information is required for the other service provider?
    - Is there a particular format that would be best?
7. **Right to object – they would like to object to how PEAS is processing their data**
    - Can you provide some additional context; what type of processing are you objecting to? My colleague will contact you to ask for more information.
8. **Rights related to automated decision making – they would like to talk about how PEAS uses automated processing for decision making**
    - At present, PEAS does not use a computer-based analysis for profiling, and therefore restrictions are not necessary do not apply.

Immediately after the call

Take all the information collected and send in an email to dataprotection@peas.org.uk.

- Please make sure you also include the time and date of the call – to ensure PEAS can comply with our GDPR requirements accordingly.

Appendix C: Service providers compliance with GDPR

***work in progress*

PEAS' compliance with GDPR cannot be ensured by simply picking GDPR-compliant service providers, however it is our responsibility to ensure that our service providers are compliant with GDPR in how they deliver their services.

Service Provider	Compliance with GDPR	Relevant link	Last Checked
Data Storage			
Mailchimp *(forms)*	Updated Privacy Policy to be GDPR compliant for EU	Mailchimp Privacy Policy updated 23/05/18	25/05/2018
Salesforce *(contact database)*	Yes	Salesforce Privacy Policy 24/05/18	25/05/2018
Google *(email, Youtube and file storage)*	Already implemented strong privacy protections	Our commitment to GDPR	05/05/2018
Dropbox *(file storage)*	Security practices already comply with the most widely accepted IT security standards and regulations, and will be fully compliant by May 25th 2018	Dropbox's GDPR compliance journey	05/05/2018
Online Platforms			
Raising IT *(website and donations)*	Making a number of changes to our product, service and processes to ensure readiness for the GDPR	What changes are Raising IT making to be compliant with the GDPR?	05/05/2018
Facebook (*social media*)	Will comply with GDPR, supported by the largest cross-functional team in Facebook's history	Facebook's commitment & preparation	07/05/2018
Twitter (*social media*)	Making updates across core product, policy and operations	Twitter's approach to privacy and the GDPR	07/05/2018
LinkedIn (*social media*)			
Wufoo (*recruitment*)	Yes	Wufoo's commitment to GDPR	25/05/2018
Processing financial information and donations			
Charities Aid (CAF)	Yes	Privacy policy	25/05/2018
BACS			
PayPal			
Xero	Yes	Privacy policy	25/05/2018
Stripe	Yes	Privacy Policy updated 25/05/18	25/05/2018
Go Cardless			
WorldPay			
RSM	Yes-New contract issued		25/05/2018
JustGiving, Virgin Money, Chuffed?			

Human Resources			
Her Majesty's Revenue and Customs (HMRC)	Yes		25/05/2018
PPS (*payroll*)	External payroll processor	New GDPR policy received	08/05/2018
Now Pensions (*pensions*)	PEAS pension provider	New supplier agreement	08/05/2018