PEAS Data Protection Policy

Introduction

PEAS is committed to protecting the privacy and security of the personal data of our students, staff, partners and supporters and adhering to the applicable data protection laws in the countries in which we work.

This policy sets out PEAS' commitments to ensuring that any personal data which PEAS processes is carried out in compliance with data protection legislation. PEAS ensures that good data protection practice is imbedded in the culture of our staff and our organisation.

This policy applies to all personal data processed by PEAS. All PEAS staff are expected to comply with this policy and failure to comply may lead to disciplinary action for misconduct.

We understand that some of the terminology can be hard to understand – as such, we have added definitions to **Appendix A – Definitions**. Alternatively, if you have any questions about this policy, please do email your question to dataprotection@peas.org.uk.

Legislation

PEAS is registered in the UK, Uganda and Zambia. Therefore, the applicable legislations are as follows:

- **UK** – UK General Data Protection Regulation tailored by the Data Protection Act 2018 – overseen by the Information Commissioner's Office, and the Privacy and Electronic Communications Regulations
- **Uganda** – Data Protection and Privacy Act, 2019 – overseen by the personal data protection office within the National Information Technology Authority
- **Zambia** – The Data Protection Act, 2021 – overseen by the Office of the Data Protection Commissioner

PEAS has conducted a review of these three pieces of legislation when developing this PEAS' data protection policy. Where the contents of the legislations differ, PEAS has adopted the strictest requirements for this policy.

Data Protection Principles

PEAS complies with the data protection principles set out below. When processing personal data, PEAS ensures that:

- it is processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
- it is collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')
- it is all relevant and limited to what is necessary for the purpose ('data minimisation')

- it is all accurate and, where necessary, kept up to date and that reasonable steps will be taken to ensure that personal data that is inaccurate is rectified or erased without delay ('accuracy')
- it is kept for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation')
- it is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures ('integrity and confidentiality')

PEAS will facilitate any request from a data subject who wishes to exercise their rights under data protection law as appropriate, always communicating in a concise, transparent, intelligible and easily accessible form and without undue delay.

Data Subject Rights

PEAS has processes in place to ensure that it can facilitate the following requests made by an individual to exercise their rights under data protection law. All requests should be sent to dataprotection@peas.org.uk.

Subject access: the right to request information about how personal data is being processed, including whether personal data is being processed, the purpose of processing that data and the right to be provided with a copy of that data. PEAS will respond to this request within 7 days.

Rectification: the right to allow a data subject to rectify inaccurate personal data concerning them. PEAS will respond to this request within 7 days.

Erasure: the right to have data erased and to have confirmation of erasure, where:

- the data is no longer necessary in relation to the purpose for which it was collected, or
- where consent is withdrawn, or
- where there is no legal basis for the processing, or
- there is a legal obligation to delete data

PEAS will respond to this request within 7 days.

Restriction of processing: the right to ask for certain processing to be restricted in the following circumstances:

- if the accuracy of the personal data is being contested, or
- if our processing is unlawful but the data subject does not want it erased, or
- if the data is no longer needed for the purpose of the processing but it is required by the data subject for the establishment, exercise or defence of legal claims, or
- if the data subject has objected to the processing, pending verification of that objection

PEAS will respond to this request within 14 days. If PEAS decides not to comply with the request from a Ugandan citizen for any reason, the Ugandan personal data protection office must be notified within 7 days.

Data portability: the right to receive a copy of personal data which has been provided by the data subject in a structured format. PEAS will respond to this request in 30 days.

Automated Profiling: PEAS does not use automated or computer-based techniques to make significant decisions about individuals based on their personal information. If PEAS intended to start automated profiling, then data subjects would be notified and would have the opportunity to respond.

Data about children: As an international child-centred organisation, PEAS has a commitment to promoting the rights of all children. As a school network operator, PEAS processes a range of personal information about children and has prioritised data protection in the design of our school information system, which is the key place where all school-level data is scored. PEAS gathers consent from guardians whilst collecting data about our students, and PEAS does not use this data for any marketing purposes. Further information on this is provided in the 'Collection of personal information' section below.

Complaints: Data subjects have the right to submit a complaint relating to PEAS' handling of data subject requests. Data subjects can complain to PEAS by emailing dataprotection@peas.org.uk. Alternatively, data subjects may choose to submit a complaint to the relevant authority as follows:

- **UK** – Submit complaints to the Information Commissioner's Office by phone 0303 123 1113 or through this form;
- **Uganda** – Submit complaints to the National Information Technology Authority through this form;
- **Zambia** – Submit complaints to the Office of the Data Protection Commissioner – process is yet to be publicised.

Collection of personal information

This refers to the lawful bases by which PEAS collects personal information:

Consent

In Uganda and Zambia, PEAS operates networks of secondary schools and is directly educating over 15,000 students every year. In order to operate these schools, PEAS processes a range of personal information about students and staff. PEAS gathers consent from guardians and staff members at the point of collecting the personal information, and ensures all data is stored securely on PEAS' school information management system and our online document repositories. Access to personal information is restricted to ensure the integrity of the data, and any insights are reported at overall school or network level – without any personal information about individual students or staff.

PEAS also works with non-PEAS schools through our System Strengthening programmes, where PEAS works in partnership with government and other education operators. Although PEAS collects a range of data about these partner schools in order to tailor support and measure improvements over time, PEAS does not collect personal data about individual students in partner schools.

In the UK, PEAS gathers consent for our mailing list 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.

Legitimate interests

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 interest 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 will oblige.
- For the purposes of direct marketing to a supporter of the organisation. The supporter will always have the option to opt-out of direct marketing, through unsubscribing or requesting that their information be deleted. This does not apply for electronic marketing, which is instead regulated by the Privacy and Electronic Communications Regulations (see electronic marketing section below).

PEAS may use legitimate interest in other circumstances, where there is a clear and specific purpose which does not infringe on the rights and freedom of the individual.

Electronic marketing

In the UK, PEAS will only use electronic marketing, through email or text messages, where the individual has provided specific consent to be contacted.

Necessary to fulfil a contract

The processing of data can be necessary in relation to contract which the data subject enters 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.

Data Breaches

PEAS recognise that in this modern age where charities are sadly targeted by cyber criminals, it is not possible to completely remove or avoid the risk of data breaches.

As part of PEAS' commitment to protecting the privacy and security of personal data, PEAS has established a range of controls to detect and respond to data breaches. PEAS has a responsibility to report certain types of personal data breach to the applicable authority (within 24 hours - 72 hours of becoming aware of the breach, dependent on the country). 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.

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 **Error! Reference source not found.** as a key component to avoiding breaches.

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 via the internal reporting channels without delay for further investigation. PEAS has conducted training on recognising and reporting data breaches through an internal data breach 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 a large volume of content is deleted from Office 365. In these cases, the PEAS COO will be notified without delay for further investigation.

Reporting and responding to breaches

Once a breach has been detected, PEAS COO is notified and the breach is assessed to identify the scope of the breach, the risk likelihood and severity and any measures to mitigate any possible adverse effects. Based on this, PEAS COO co-ordinates immediate measures to minimise impact (e.g. the remote wipe of devices or restricting access to files) and reports based on the following criteria:

- **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.
- **Depending on the risk, notify the relevant authority & the Board**. If the breach is likely to result in a risk to people's rights and freedoms, then the relevant authorities must be notified within 24 hours - 72 hours[1] of becoming aware of the breach and the PEAS Board of Trustees will be notified[2] simultaneously.
- **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.

[1] Exact time period is dependent on the location of the data subjects – Zambia legislation requires the data breach to be reported to the Office of the Data Protection Commissioner within 24 hours, whilst UK legislation requires the data breach to be reported to the Information Commissioner's Office within 72 hours.
[2] The Communications Policy will also be attached, which outlines PEAS' Crisis Response Plan.

PEAS will investigate and document every data breach and identify any measures that should be taken to mitigate the impact and minimise the risk of the breach reoccurring.

PEAS has also developed a cyber incident response plan, to help co-ordinate PEAS' response in case of a severe cyber security incident.

Governance

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.

In practice, PEAS' COO is the PEAS Global Data Protection Officer and has overall responsibility for data protection on PEAS' GST, working closely with various teams on implementation.

The Heads of Operations are Data Protection Officers in each country – to ensure each country office is adhering to PEAS data protection policy, to monitor compliance with the applicable legislation and to be PEAS point of contact with the applicable authority.

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. All staff must read, understand and comply with this policy when processing personal data on PEAS' behalf and attend training on its requirements.

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.

Key documentation

PEAS has put in place and collected a range of documentation to ensure compliance with the data protection policy and associated legislation. The key documentation can be summarised as followed:

Data Protection Policy

This policy details PEAS' approach to ensuring the protection of personal information held by PEAS, in accordance with the applicable legislation in UK, Uganda and Zambia. The policy details 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.

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.

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.

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.

PEAS Data Breach Record

PEAS has designed a data breach reporting framework to support employees in reporting any data breach, which in turn alerts the PEAS COO. The PEAS Data Breach Record maintains a record of all data breaches and steps PEAS has taken to address the breach.

Evidence

PEAS must record measures taken to comply with the data protection legislations, in order to demonstrate that we are compliant. 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: Definitions

- **'automated profiling'** is defined as any form of automated or computer-based processing of personal data used to make significant decisions about a person.
- **'COO'** refers to PEAS' Chief Operating Officer – who sits in the UK team and is also PEAS' Data Protection Officer.
- **'data breach'** is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration or access to personal data.
- **'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.
- **'data protection officer'** is an individual within the organisation who is responsible for ensuring that the organisation applies the legislations and policy when processing personal data.
- **'GST'** refers to PEAS' Global Strategy Team – the over-arching leadership committee in PEAS, responsible for day-to-day decision making.
- **'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.
- **'processing'** is defined as any operations performed on personal data, whether or not by automated means, such as collection, recording, storage and retrieval.

Appendix B: Service providers compliance with UK GDPR

As part of PEAS' commitment to protecting the privacy and security of personal data, PEAS has reviewed each third-party service providers to check their adherence to global data protection best practice in how they deliver their services.

Service Provider	Compliance with UK GDPR	Relevant link	Date verified
Data Storage			
Mailchimp *(forms)*	Updated Privacy Policy to be GDPR compliant for EU. Signed up for the UK GDPR register.	Mailchimp Privacy Policy updated 23/05/18	25/05/2018
Salesforce *(contact database)*	Yes - signed up for the UK GDPR register.	Salesforce Privacy Policy 24/05/18	25/05/2018
Google *(email, Youtube and file storage)*	Already implemented strong privacy protections. Signed up for the UK GDPR register.	Our commitment to GDPR	05/05/2018
Office 365 *(file storage, productivity apps)*	Compliant with the UK Data Protection Act.	Office 365 's GDPR compliance journey	23/07/2022
Online Platforms			
WordPress	Yes, as of WordPress 4.9.6, the WordPress core software is GDPR compliant.	Automattic (owner of WordPress) statement	26/08/2022
Facebook (*social media*)	Will comply with GDPR, supported by the largest cross-functional team in Facebook's history. Signed up for the UK GDPR register	Facebook's commitment & preparation	07/05/2018
Twitter (*social media*)	Making updates across core product, policy and operations. Signed up for the UK GDPR register.	Twitter's approach to privacy and the GDPR	07/05/2018
LinkedIn (*social media*)	Signed up for the UK GDPR register	Learn more about GDPR with LinkedIn	26/08/2022
Wufoo (*recruitment*)	Complying with GDPR.	Wufoo's commitment to GDPR	25/05/2018
Processing financial information and donations			
Charities Aid (CAF)	Yes. Signed up for the UK GDPR register.	Privacy policy	25/05/2018
BACS	Signed up for the UK GDPR register		
PayPal	Signed up for the UK GDPR register	Privacy Statement	04/08/2022
Xero	Yes. Signed up for the UK GDPR register	Privacy policy	25/05/2018
Stripe	Yes. Signed up for the UK GDPR register.	Privacy Policy	25/05/2018

Go Cardless	French owned business so complied with the EU GDPR.	GDPR Terms of Service	24/11/2022
WorldPay	Signed up for the UK GDPR register.	Privacy Policy	24/11/2022
JustGiving, Virgin Money, Chuffed	Signed up for the UK GDPR register.		
Donorbox.org	Payment processor Stripe is compliant – and provides guidance on GDPR compliant forms	Is Donorbox GDPR compliant?	24/11/2018
Human Resources			
Her Majesty's Revenue and Customs (HMRC)	Yes.	HMRC Privacy Noticev	25/05/2018
PPS (*payroll*)	External payroll processor . Signed up for the UK GDPR register.	New GDPR policy received	08/05/2018
Now Pensions (*pensions*)	PEAS pension provider. Signed up for the UK GDPR register.	New supplier agreement	08/05/2018
Breathe	Achieve GDPR-compliance through Breathe.	Data protection	24/11/2022
Myepaywindow.com	Signed up for the UK GDPR register under the company name Netcraft.	Netcraft Privacy Policy	24/11/2022

Appendix C: Crisis Response Plan

In the case of a severe Cyber Security breach, where access to all of PEAS' systems have been lost.

This document page is to be saved offline by the key emergency contacts listed below.

Cyber incident contacts:

In the case of a severe cyber breach, the following individuals will be responsible for co-ordinating their country's response, contacting all PEAS employees in country and reporting back progress to the global response co-ordinator (to be nominated when a breach occurs). Multiple contacts have been selected for each country, in case one or two contacts are on leave during the incident.

- **UK** – Chief Operating Officer, Senior Manager for Operational Excellence and Administrator
- **Uganda** – Country Director, Head of Operations and IT Specialist
- **Zambia** – Country Director, Deputy Country Director – Head of Operations and MEL Assistant

If the incident has caused a loss of PEAS communication services (email, Teams, etc) then WhatsApp will be used as the primary communication channel, followed by direct phone calls.

Steps:

1. **Detect** incident and **escalate** immediately to COO.
2. Initially **categorise** the incident and identify the **severity** of the incident, to help with the next steps. Categories include:
    - **Malicious code:** Malware infection on the network, including ransomware
    - **Denial of Service:** Typically a flood of traffic taking down a website, can apply to phone lines, other web facing systems, and in some cases internal systems.
    - **Phishing:** Emails attempting to convince someone to trust a link/attachment.
    - **Unauthorised Access:** Access to systems, accounts, data by an unauthorised person (internal or external) – for example access to someone's emails or account.
    - **Insider:** Malicious or accidental action by an employee causing a security incident.
    - **Data breach:** Lost/stolen devices or hard copy documents, unauthorised access or extraction of data from the network (usually linked with some of the above).
    - **Targeted attack:** An attack specifically targeted at the business - usually by a sophisticated attacker (often encompassing several of the above categories).
3. Contact **PEAS cyber incident contacts** across all offices to gauge: are they facing the same issues, who is facing them and what is the impact?
4. Consider whether the incident has to be **reported**, as follows:
    - First, escalate to **PEAS COO and CEO** – who then decide further escalations (e.g. to Police – assume we wouldn't want to wait on the Board for this)
    - **PEAS Board** – to be informed either within 24 – 72 hours, depending on the nature of the breach.
    - **Police** - charities who are currently suffering a live cyber-attack (in progress) should call 0300 123 2040 immediately (available 24 hours a day, 7 days a week).
    - **NSCS** - Once reported to the Police, can report to the National Cyber Security Centre via https://report.ncsc.gov.uk/. NSCS can support technical advice on how to respond to a live incident.

- **ICO** – If there has been a material data breach of personal data, this should be reported to the Information Commissioner's Office within 72 hours via calling +44 303 123 1113.
- **Charity's Commission** – Significant data breaches or cyber-crime incidents must be reported to the Charity's Commission. It is up to PEAS' Trustees to determine whether an incident is sufficient and should be reported via https://register-of-charities.charitycommission.gov.uk/report-a-serious-incident.

5. Follow-through with case management protocol, including taking steps to:

   - Maintain **an incident log**, and store any evidence or materials which may be needed for ensuing legal action.

1. **Analyse** the impact of the incident, including an assessment across all of PEAS' areas of operation to ascertain the severity of the incident and the number of users affected, identifying which systems have been affected, identifying the data that is at risk and the sensitivity of that data. This should consider a review of the **current status of all key systems** (computer devices, mobile devices, email, Teams, Sharepoint & OneDrive, public website, social media channels, payment websites, bank accounts, Quickbooks and Salesforce).

   - **Reduce the impact**, such as:
     - Removing individual's access to PEAS systems through disabling them on Office 365 admin panel;
     - Disabling internet network access for any computers known to be affected;
     - Pushing out security patches to all devices, to prevent further breaches;
     - Updating all passwords for affected PEAS systems;
     - Proactively post a holding message on PEAS' social media channels, if access to all PEAS systems has been lost;
     - Identify and secure any back-ups of data.
   - Taking steps to **recover and restore** systems and data.
   - Completing a **post-incident report** to evaluation PEAS' response to the incident and identify lessons learned for the future, using the following template:

Incident Overview	
Date of Incident	
Risk Level (L/M/H)	
What happened?	
Who/what identified the risk?	
How long did it take PEAS to respond to the incident?	
Who was the incident response leader?	

Detail how was the incident resolved?	
Evaluation	
Was the response effective?	
What was effective?	
What could have been better?	
Are there security improvements which could have prevented the incident, or enabled earlier detection?	
Was there data which could have been useful but wasn't available?	
Did the processes and communications work well?	