Data Protection Policy

Effective 25th May 2018

Version 1.0

Purpose

Data Protection law in the UK is changing. This policy will ensure that The Pony Club can both comply with the new law and continue to work effectively.

Terminology

Some specialised terms are introduced in italics and defined briefly in a glossary, which is appended to this policy.

The new law

The EU-wide *General Data Protection Regulation* (GDPR) is incorporated into British law from 25th May 2018, replacing the *Data Protection Act* (1998). The aim of the GDPR is to protect the *personal data* of all EU citizens. (Brexit does not affect this. The UK data protection legislation, being twenty years old, was overdue for revision in any case.)

GDPR confers rights on *data subjects* and imposes obligations on *data controllers*.

By keeping their personal data safe, GDPR compliance will protect the interests of Pony Club staff, volunteers and above all the approx. 36,000 members whose details are held on its computer systems and in paper records.

Effectiveness: the use of personal data

The Pony Club depends personal data, to operate effectively. As a membership organisation, we rely on accurate records of our members to invite people to meetings and events, collect subscriptions and provide information to them. As a sports organisation, we need both membership data and event entry forms to run our rallies and competitions. As an organisation with young members, we have paramount duties for safeguarding children and for promoting health and safety, which again depend on keeping accurate records with appropriate privacy and security.

So: this policy is designed to be workable, as well as compliant. It does not, for example, require explicit individual consent for activities which are already permissible under the legislation under the so-called *Legitimate Interests* basis for our day-to-day operations.

Does this policy apply to everyone at Pony Club?

Yes. Any person or organisation who undertakes *data processing* (a data controller) must comply with GDPR. For The Pony Club, this includes both staff and volunteers throughout our organisation, including Areas, Branches and Centres.

Who is accountable and responsible for this policy?

Ultimately, the Board of Trustees is accountable for compliance across The Pony Club.

The Senior Management Team (SMT) is responsible for the operation of this policy. It has appointed a *Data Protection Lead* (DPL, currently Kate Shaw, Finance Director) to lead on the implementation and monitoring of the policy. The DPL will be the point of contact for data protection and privacy enquiries from staff, volunteers, members, parents or guardians and the general public (and also for any official or media enquiries).

The *Information Commissioner's Office* (ICO) oversees DPA and GDPR compliance. The Pony Club is registered with the ICO as a data controller (registration number Z6167202). The Pony Club is obliged to notify the ICO of any significant data protection incident. Any such notifications will be managed by the DPL and made known to the SMT and Board.

Data subjects have legal rights

The Pony Club respects the legal rights of individuals whose personal data it holds:

- The right to be informed (satisfied through the issue of a *Data Privacy Notice*)
- The right of access (allowing an individual to raise a *Subject Access Request*)
- The right to rectification (if our record is wrong, we must correct it on request)
- The right to erasure (also known as 'the right to be forgotten')
- The right to restrict processing (e.g. pending data rectification)
- The right to object (primarily to opt out of all direct marketing)
- The right of data portability (more relevant to e.g. banks or phone companies)

Lawful basis for data processing

We can only process personal data with a *lawful basis*, six of which are defined in GDPR.

1. Where we have explicit consent from the person. Explicit consent can be provided, for example, via 'Opt-in' tick boxes on a membership, entry or registration form.
2. Where it is a legal obligation. This will be rare, but if you are legally obliged, for example by a police officer, to share someone's details, then you must do so.
3. Similarly, if it is in the individual's vital interests. For example, in the event of an accident you should share details of the injured party with the medical team.
4. Where the data are necessary to perform a contractual obligation. This would typically be to supply goods or services ordered by a Pony Club member.
5. When it is in the legitimate interests of The Pony Club, or of the data subject. This is a wide-ranging and useful provision, covering most of the day-to-day activities of a membership organisation such as The Pony Club.
6. When it is necessary to undertake a public task. (This is unlikely to apply.)

The Pony Club maintains an *Information Asset Register* which includes the lawful basis appropriate to each regular data processing activity, with *Legitimate Interests Assessment* (and/or *Data Privacy Impact Assessment*) where necessary to establish that basis.

Data retention

The Pony Club must keep some personal data for an extended period, after the individuals (data subjects) involved have left The Pony Club. This may be for legal or audit reasons, but also for various other purposes, for example to provide employment references.

Pony Club will not keep personal data for longer than is necessary. This means that data will be deleted when no longer required, as set out in a data retention schedule.

The Pony Club's corporate responsibilities

The Pony Club commits to:

- Implement this policy and ensure it remains compliant with legislation.
- Ensure that appropriate technical and organisational measures are taken against unlawful or unauthorised processing of personal data, and against *data breach*.
- Give appropriate guidance and training to Pony Club employees and volunteers.
- Maintain an information asset register, including lawful basis for data processing.
- Devise and implement an appropriate data retention schedule.
- Handle properly any queries, subject access requests or complaints that may arise.
- Consider risk in its data processing activities.
- Keep records on data processing practices and information security measures.
- Cooperate with the ICO and name a contact point (the DPL).

Your personal responsibilities

As a volunteer or member of Pony Club staff, if you process personal data you must:

- Follow this policy and related procedures whenever personal data is being used.
- Think about why you need to handle personal data and minimise its use.
- Reduce as much as possible the likelihood of a data breach, by maintaining information security in line with this policy and any related Pony Club procedures.
- Report any data breaches to the DPL immediately on discovery.
- Ensure that personal data is managed according to its data retention schedule.
- Inform your line manager (or Area Representative) and the DPL immediately if you receive a request from a data subject for information held about them (a Subject Access Request), or a similar request for e.g. rectification, or any complaint.

Area, Branch and Centre responsibilities

Don't panic! The key point is to make sure that you don't lose or misuse data. You also need to make sure that personal details are properly stored and looked after and that you are only using data for the purposes of which people are aware. The Pony Club office will issue guidance on data storage to the Areas, Branches and Centres.

It is helpful to identify someone to take charge of Data Protection issues at local level. Typically, this responsibility might lie with a Membership Secretary or similar officer.

If you carry out local data processing of any sort outside the general procedures of The Pony Club, you should consider the lawful basis for doing so –this would normally be Consent or Legitimate Interests –and ensure that information collected is the minimum necessary, is held securely, and is deleted when no longer required.

You must operate within this Data Protection Policy and you should also publish a Data Privacy Notice (DPN). GDPR creates certain obligations about what should be included in a DPN: The Pony Club office will issue guidance and a suitable DPN template for your use.

If you share data with a third party, you should have a Data Sharing Agreement in place (to ensure that both parties' use of the data will remain GDPR-compliant).

Key points for local data collection

- You must be very clear to members about what you are doing with personal data when you collect it. An example might be for use at a Pony Club Camp. Attaching the standard Data Privacy Notice to the form would be the usual way to do this.
- If you require someone's consent to process their personal information, they must actively give it to you and you must note it. Implied consent is no longer sufficient (application form tick boxes should be opt-in, not opt-out).
- You must only collect relevant personal information that you need for the purpose in hand. Such information might include name, address, age etc. You should not capture irrelevant information (e.g. gender, unless it is genuinely required).
- You must only keep information for as long as you have a continuing need for it.
- You must keep personal information as secure as possible to prevent loss, damage, theft or unauthorised disclosure.

What to do if things go wrong

Any breach of this Data Protection Policy or GDPR requirements must be reported to The Pony Club's Data Protection Lead. This is to safeguard both individuals and the Pony Club, and to limit potential damage from information loss.

If in doubt as to whether an incident is significant, please refer to Marty Bibby for advice.

Further information, references and acknowledgements

For any further information, please contact Marty Bibby at the Pony Club office.

Additional advice is available from the Information Commissioner's Office.

https://ico.org.uk/for-organisations/charity/charities-faqs/

https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources/

The wealth of material on data protection on the website of Girlguiding UK is useful for background information and has influenced the development of this Pony Club policy.

Appendix: Glossary

Some of these definitions are simplified for clarity. For more detail, visit the ICO website.

Data Breach		The loss, destruction, erasure or alteration of personal data; or the unauthorised disclosure, sharing, use or publication of personal data.
Data Controller		A legal 'person' (typically, meaning an organisation) who determines why and how personal data are processed.
Data Privacy Notice	DPN	A straightforward, public statement of how an organisation applies data protection principles to processing personal data.
Data Processing		The use, collection, storage and disposal of personal data. This includes, for example, sharing information by email.
Data Protection		Ensuring that data (particularly personal data) are kept accurately and securely.
Data Protection Act	DPA	UK legislation (dating from 1998) that preceded GDPR.
Data Protection Impact Assessment	DPIA	A formal assessment of the impact to data subjects of certain high-risk data processing (generally unlikely to apply to the Pony Club).
Data Protection Lead	DPL	The person appointed by the Pony Club to oversee its data protection duties.
Data Subject		A living individual whose personal data is known to the data controller. This may mean a member, volunteer or others such as coaches and officials at Pony Club events.
General Data Protection Regulation	GDPR	EU-wide data protection legislation, effective in UK law from 25 May 2018.
Information Asset Register	IAR	A record of which data are held, where and how those data are processed in accordance with GDPR standards.
Information Commissioner's Office	ICO	The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Lawful Basis		One of six allowable reasons to process personal data, as set out in GDPR: Consent, Contract, Legal obligation, Vital interests, Public task, Legitimate interests.
Legitimate Interest Assessment	LIA	A formal assessment of whether the Legitimate Interests lawful basis is appropriate for a particular activity.
Personal Data		Data relating to a living individual who is, or can be, identified from the data (or from using the data along with other information that is known to the data controller).
Subject Access Request	SAR	The exercise of an individual's right to obtain a copy of their personal data.