Data Privacy Management Procedure
for Pennine District

Issue 1 Draft 1 : March 2018

About this procedure

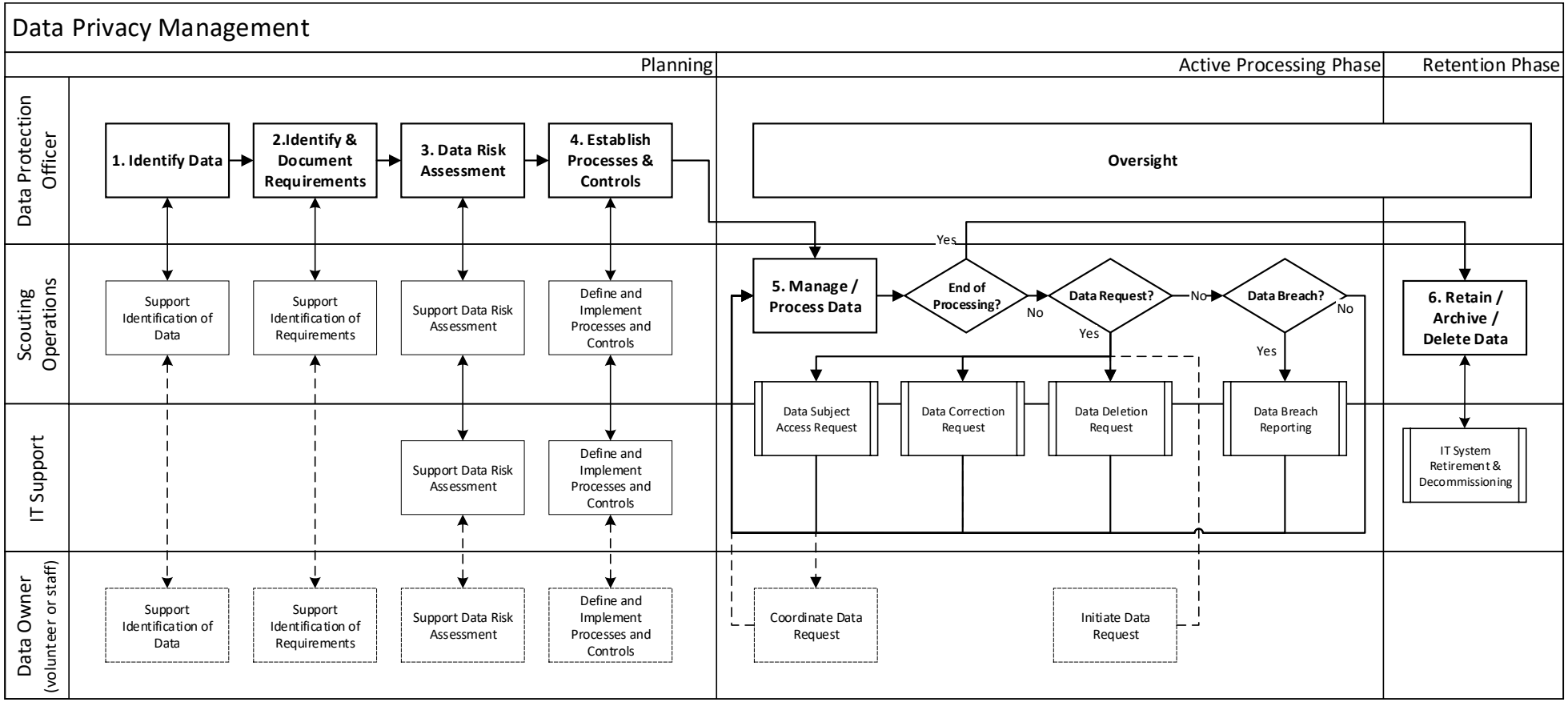
This procedure defines how Pennine District will manage personal data to assure appropriate data privacy in accordance with the UK Data Protection Bill 2017. It should be read in conjunction with current information and guidance published by the UK Information Commissioner's Office (ICO – http://ico.org.uk/)

Note that once the UK leaves the European Union, additional requirements of the European Union General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) may continue to apply with respect to data processed relating to EU citizens, which may include some youth members and volunteers. As Pennine District does not regularly process data relating to citizens of the EU as a matter of course, it is considered that the UK Data Protection Bill 2017 will meet the requirements of the EU GDPR regulation. Should this position change this procedure will be reviewed.

The general requirements for data protection are defined in the Pennine District Data Protection Policy.

The general process for assuring data privacy is shown overleaf. This is supplemented by four additional procedures:

- Subject Data Access Request Procedure
- Subject Data Correction Request Procedure
- Subject Data Deletion Request Procedure
- Subject Data Breach Reporting Procedure



This process is described in more detail below

Step	Description
1. Identify Data	The Data Protection Officer is responsible for identifying all personal data, supported by the appropriate Responsible Officer (data owner) and other appropriate volunteers in Pennine District. For each set of personal data processed, the Pennine District data protection policy defines: • The data description • The personal data included • How and where data is stored • The data retention policy • The Responsible Officer (data owner) Where new data sets or changes to datasets (including data no longer held) are identified, the data protection policy should be updated to reflect the changes and steps 2 – 4 (and possibly step 6) repeated for the dataset
2. Identify and Document Requirements	For all personal data, the Data Protection Officer is responsible for identifying data protection and data privacy requirements, supported by the appropriate Responsible Officer (data owner) and other appropriate volunteers. These are generally based on the requirements derived from the UK Data Protection Act 2017. Where changes to personal datasets are identified (step 1 above) additional data protection/privacy requirements may be identified to comply with applicable jurisdictional requirements. Any additional such requirements should be documented.
3. Data Risk Assessment	The Data Protection Officer is responsible for ensuring that data privacy risks are identified, supported by the appropriate Responsible Officer (data owner) and appropriate Pennine District volunteers and/or officers. Based upon the data identified in step 1 above and the requirements identified in step 2 above, data privacy risk assessments should be conducted to identify applicable processes and controls. Pennine District has determined that a general privacy impact assessment is required. This is documented in annex 1 below and general processes and controls have been considered to mitigate the risks identified in this generic privacy impact assessment. Such processes and controls have been developed in consideration of the general privacy impact assessment and implement established data protection / privacy good practices. It is not considered necessary to document detailed risk assessments where such good practices are followed. Specific risk assessments (in the form of data, system or platform specific privacy impact assessments) may be conducted and documented for specific data privacy requirements. See ICO guidance for examples of suitable data privacy impact assessments.
4. Establish Process and Controls	General data protection principles and controls are defined in the Pennine District data protection policy. General data privacy process and controls are defined in the following procedures: • Subject Data Access Request Procedure • Subject Data Correction Request Procedure • Subject Data Deletion Request Procedure • Subject Data Breach Reporting Procedure Where changes to personal datasets are identified (step 1 above), and/or where specific data privacy impact assessments are conducted the applicability of these general

Step	Description
	requirements, processes and controls should be reviewed to ensure that they are fully applicable. Where existing requirements, processes and controls are considered insufficient to assure data protection/privacy one of the following must occur: • Update processes and controls to include new requirements and mitigate risks • Implement specific (additional or alternative) processes and controls to meet specific requirements and mitigate specific risks
5. Manage / Process Data	Data processing will take place following defined processes and established practices and in accordance with the data protection measures defined in the Pennine District data protection policy. Any specific data privacy management actions will be conducted in accordance with the following procedures: • Subject Data Access Request Procedure • Subject Data Correction Request Procedure • Subject Data Deletion Request Procedure • Subject Data Breach Reporting Procedure In addition, the following rights must be respected: **Right to Object** Individuals should be informed of their right to object to data processing at the first point of communication i.e. the first email they receive, available on their first visit to a website etc. Individuals may object to: • Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); • Direct marketing (including profiling) e.g. Moor House Adventure Centre mailings • Processing for purposes of scientific/historical research and statistics. In these cases, processing must cease unless the Pennine District can demonstrate • Compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual (e.g. safeguarding of young people or compliance of other regulatory requirements) • the processing is for the establishment, exercise or defence of legal claims Objections to direct marketing must be acted upon immediately **Right to Restrict Processing** Process should be halted when a data subject as a legitimate right to block processing. During this 'block', data may be stored but not processed. Sufficient data should be retained to identify the block. This is applicable when: • An individual contests the accuracy of the personal data, processing should be restricted until we have verified the accuracy of the personal data. • An individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether Pennine District's legitimate grounds override those of the individual.

Step	Description
	• When processing is unlawful and the individual opposes erasure and requests restriction instead. • If the Pennine District no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim. **Right to Data Portability** Data subjects may request a copy of their personal data portability when: • They have provided to their personal data to the Pennine District; • The processing is based on the individual's consent (or for the performance of a contract); and • when processing is carried out by automated means. Data should then be provided to the data subject (or transmitted to another data controller) in an open format e.g. .csv file, .txt file etc, without undue delay and within one month, unless the data is considered complex (see Annex 2)
6. Retain / Archive / Delete Data	Following the ending of active processing a decision will be made to either retain, archive or delete data as follows: • Retain data: For cases where data is no longer being actively updated, changed or added to, but which still needs to be referred to on a regular basis. Where this is the case, access controls and permissions should be updated to make data 'read only' where possible • Archive data: For cases where data is no longer being actively updated, changed or added to, and which does not need to be referred to on a regular basis (i.e. may be retained for statutory purposes, risk mitigation purposes etc). Where this is the case, access controls and permissions should be updated to make data 'read only' where possible and the data should be moved to a suitable secure hard copy of electronic archive • Delete data: For cases where data no longer needs to be retained When considering the above it should be recognised that data may progress through a natural life cycle (active processing ➔ retained ➔ archived ➔ deleted), possibly bypassing these steps. Data should not be retained beyond the retention period defined in the Pennine District data retention policy

Annex 1 – General Data Privacy Impact Assessment

Pennine District has determined the need for a Data Privacy Impact Assessment (PIA). This is because Pennine District:

- Collects new information about individuals, including data of a kind particularly likely to raise privacy concerns or expectations e.g. health records, criminal record checks or other information that people would consider to be private.
- Requires individuals to provide information about themselves
- May use information about individuals for a purpose it is not currently used for, or in a way it is not currently used
- Discloses information to third parties (legal and natural persons) who are part of the Scout Association or other statutory bodies, where there is a need to disclose such information to assure the safety or safeguarding of our members, staff or members of the public, or to manage complaints.
- May take action against individuals based on personal data, which may have an impact in their employment or appointment status

Pennine District does NOT

- Collect information about or contact individuals in ways that they may find intrusive
- Disclose any other personal information to organisations or people other than as described above
- Use technology that might be perceived as being privacy intrusive e.g. the use of biometrics or facial recognition.
- Take action against individuals in ways that can have a significant impact on them, other than as described above

As a result of the above, the general data privacy risk assessment has been conducted:

Privacy Issue	**Risks to Individuals**	**Compliance Risk**	**Associated organisational risk**
Data inaccuracy	Right to be informed Right of access Right to rectification Right to object Right to data portability Right to erase Right to restrict processing	Inability to comply with applicable requirements of UK Data Protection Act 2017 (and EU GDPR) Inability to comply with Policy, Organisation and Rules of the Scout Association	Financial penalties Other enforcement actions Reputational risk
Data breach	Data confidentiality		
Data destruction	Right of access Right to object Right to data portability Right to erase		
Data retention and processing beyond defined period	Right to restrict processing		

In seeking to mitigate such risks, specific controls have been identified and documented in the District data protection policy.

Annex 2 – Complex Data Portability Requests

Pennine District considers the following data subject portability requests to be complex. Where this is the case, acknowledgement of the request should be provided to the data subject within 30 days of receiving the request and the data should be provided to the data subject (or an alternative data controller) as soon as possible, and always within 90 days of receiving the request.

- Any request involving multiple data stores from within the Pennine District Office 365 environment (e.g. email accounts, OneDrive folders, SharePoint sites [lists, folders, databases])
- Any request involving a Pennine District Office 365 data store and any other system (e.g. OSM, Compass membership database etc)
- Any request involving data held by Pennine District volunteers in personal (secure) storage locations

All other such requests are considered simple and the data should be made available or transferred within 30 days of receiving the request.

If in doubt, the Data Protection Officer, balancing the rights of the data subject and the ability of the Pennine District to transfer the data, will provide a definitive determination of whether a data transfer request is considered simple or complex.