May 2018

Data Privacy Management, Requests and Reporting Procedures

1st Howden-le-Wear Scout Group

#SkillsForLife

Scouts
1st Howden-le-Wear

Contents

About this procedure

This procedure defines how 1st Howden-le-Wear Scout Group 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 1st Howden-le-Wear Scout Group 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 1st Howden-le-Wear Scout Group Data Protection & Privacy Policy.

This Procedure Details:

– The general process for Data Privacy Management

– How we manage Data Requests; Access, Corrections and Deletions

– How we manage a Subject Data Breach

For the purpose of this document the roles identified in this procedure are fulfilled by:

– **Data Protection Officer** – Christopher Allen

– **Group Scout Leader** – Christopher Allen

– **Group Secretary** – Christopher Allen

– **Group IT Support** – Christopher Allen

– **Data Owner (Responsible Officer(s))** – Section Leaders

– **Appropriate Volunteers –** Sectional Assistants and Occasional Helper

– **Data Subject –** Individual (or their Representative)

Data Privacy Management

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 1st Howden-le-Wear Scout Group. For each set of personal data processed, the 1st Howden-le-Wear Scout Group data protection and privacy 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 1st Howden-le-Wear Scout Group volunteers and/or Leaders. 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. 1st Howden-le-Wear Scout Group 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.

Step	Description
4. Establish Process and Controls	General data protection principles and controls are defined in the 1st Howden-le-Wear Scout Group data protection and privacy policy. General data privacy process and controls are defined in the procedures that follow: • Access, Corrections and Deletions Request Procedure • 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 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 1st Howden-le-Wear Scout Group data protection and privacy policy. Any specific data privacy management actions will be conducted in accordance with the procedures follow: • Data Request; Access, Corrections and Deletions • Breach Reporting 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 1st Howden-le-Wear Scout Group 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

Step	Description
	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 1st Howden-le-Wear Scout Group's legitimate grounds override those of the individual. • When processing is unlawful and the individual opposes erasure and requests restriction instead. • If the 1st Howden-le-Wear Scout Group 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 their personal data to the 1st Howden-le-Wear Scout Group; • 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 3).
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 our data retention policy within the Data Protection and Privacy Policy

Data Requests

An individual may ask for copies of data, deletion of data or correction of data. The procedure for managing and responding to these requests is detailed below. There are some differences depending whether it is a

- Data Access Request
- Data Correction Request or
- Data Deletion Request

We have referred to these collectively as Request(s).

Step	Description
1. Data Access Request	The Data Subject makes a data subject request(s). This should be directed to the 1st Howden-le-Wear Scout Group Secretary (any member of staff or any other volunteer, including the data owner (Responsible Officer) should direct the request to the Group Secretary.
2. Accept and Acknowledge Data Access request	The Group Secretary should immediately acknowledge receipt of the data subject request. The Group Secretary should maintain a log of all requests including: • Date request received • Data subject name and contact details • Scope of data subject request • Date of request acknowledgement • Date data or data access provided This list may be consulted to determine whether a request is repetitious or malicious. The Group Secretary may, in consultation with the Data Protection Officer (if separate individuals), refuse or charge for a request as outlined above. Where the scope of the request is not specific, the Group Secretary should seek to clarify the scope of the request i.e. whether it relates to all data held by the scout group, or to a specific subset of data (specific datasets, timescales, relating to specific events etc) The Group Secretary should inform the Data Protection Officer (if separate individuals) that a subject access request has been received and the Data Protection Officer should provide support and guidance as needed. The Group Secretary should determine, with support from the Data Protection Officer, whether the data subject access request is complex or simple. If the request is considered complex (see Annex 3), the Group Secretary should inform the data subject that the request is complex and that the requested data will be provided within 90 days. If the request is not considered complex (see Annex 3), the Group Secretary should inform the data subject that the requested data will be provided within 1 month. The Group Secretary should inform the data owner(s) (Responsible Officers) of the data request.

Step	Description
3. Acknowledge Request	The data owner(s) (Responsible Officers) should acknowledge the request to the Group Secretary and prioritise their activities accordingly
4. Identify Data	Based upon the defined scope of the data subject request, the data owner(s) (Responsible Officers) should identify the specific datasets that need to be accessed
5. Identify Information Assets	Based upon the defined scope of the data subject request, and the datasets identified by the data owner(s) (Responsible Officers), the data owner(s) and Group IT Support will identify the appropriate IT Assets e.g. • Hard copy folders or file store • Office 365 datastore (e.g. email account, OneDrive folders SharePoint site and webpart [list, folder, database]) • Other system or database (e.g. Compass, OSM) Note that at this stage it may discovered that data may have been shared with third parties. Where this is the case the third party should be requested to also comply with the request and provide evidence of compliance.
6. Collate Initial Data	Using appropriate search criteria (filters, date ranges, keywords etc) derived from the scope of the data subject request, the data owner(s) (Responsible Officers) and Group IT Support will collate data and records within the scope of the request (as hard copies and/or a separate electronic copy)
7. Redact Data	The data owner(s) (Responsible Officers), assisted by the IT Support will generate and retain evidence of the data request being made. This will typically include: • A copy of hardcopy data that has been requested • A copy of electronic data that has been requested • Before and after screen shots of the requested data The data owner(s) (Responsible Officers), assisted by the IT Support will then redact the collated data and records to remove: • Any personal data which breaches the rights or freedoms of any other natural person (attention should be paid to the potential for other personal data to be reconstructed or inferred from pseudonymised data e.g. natural persons to be identified or inferred by a combination of their scouting role and home postcode) • Any data which does not directly relate to the scope of the data request and which is considered sensitive or confidential Data should be redacted in such a manner that ensures that redacted data cannot be reconstructed e.g. redacted on hard copies using a black marker pen and recopying/scanning, overwriting electronic data with null data values, deleting metadata etc.
8. Prepare Evidence Package	The data owner(s) (Responsible Officers) should prepare the necessary evidence package. This should be in a human accessible format (hard copy or electronic copy which is readable through readily available software e.g. PDF readers). Data should be

Step	Description
	organised in a logical order (e.g. dataset type, date order etc) although it is not necessary to provide a complete index or search facility.
9. Supply Data Package	The data owner(s) (Responsible Officers) should supply the data package to the Group Secretary in a suitable format (usually a hard copy folder with all contents secured, or a secure electronic store to which suitable access can be granted e.g. through the use of a temporary, read only Group account and User ID).
10. Supply Data Package	The Group Secretary should supply the data package to the data subject in a suitable format as defined above, and request acknowledgement of receipt from the data subject. A record of transmittal should be retained and the data subject access request log updated.
11. Receive Data Package	The data subject receives the data package (or access to the data package) and should acknowledge receipt. Any subsequent request broadening the scope of the original request may be reconsidered as unfounded, excessive or repetitive as described above.

Data Breach

This procedure defines how 1st Howden-le-Wear Scout Group will manage personal data breaches. Note that any sub processors engaged on behalf of 1st Howden-le-Wear Scout Group (e.g. Online Scout Manager, Microsoft, etc) are required to report ALL data privacy breaches. They should be considered as reporting parties with respect to this procedure.

Step	Description
1. Data Breach Suspected / Reported	The data subject, or any other party reports a suspected or actual personal data breach. All volunteers of 1st Howden-le-Wear Scout Group have a responsibility to immediately report any actual or suspected data breach. Failure to do so may result in disciplinary action being taken. These should be reported to the Data Protection Officer. Any volunteer receiving such a report should request the reporting party to report the matter to the Data Protection Officer and copy the Group Scout Leader with all further correspondence.
2. Acknowledge Data Breach Investigation Initiated	Upon receiving any report of an actual or suspected data breach, the Data Protection Officer will initiate an investigation and will acknowledge that the investigation has been initiated to the reporting party. All such investigations will be logged, including • Time and date of suspected breach being reported • Whether or not an actual breach occurred • Whether or not any breach was reportable (and if not, why not) • When the breach was reported

Step	Description
	If further information is required (scope, nature, time/date and suspected cause of the actual or suspected breach) this will be requested from the reporting party. Note that if the reporting party is NOT the data subject, the data subject may not be notified at this stage. The appropriate Data Owner (Responsible Officer) should be informed of the actual or suspected breach. The Group Executive Committee and District Commissioner should also be informed.
3. Identify Data	The Data Owner(s) (Responsible Officers) will identify the scope of the actual or suspected data breach. The Group IT Support will provide support to identify the IT and information assets potentially involved.
4. Data Breach Investigation	The IT Support will provide support to identify the IT and information assets potentially involved. The Data Owner(s) (Responsible Officers) and the Group IT Support, assisted by other volunteers as required, will investigate the data breach to determine whether or not there has been a data privacy breach. The following definition of a personal data breach should be considered. *"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."* For data privacy to have been breached it must affect the confidentiality, integrity or availability of personal data (relating to a natural individual) which involves e.g.: • Access by an unauthorised third party; • Deliberate or accidental action (or inaction) by a controller or processor; • Sending personal data to an incorrect recipient; • Computing devices containing personal data being lost or stolen; • Alteration of personal data without permission; or • Loss of availability of personal data Where possible, immediate steps should be taken to halt or minimise the scale of the data breach.
5. Receive Investigation Summary	If personal data privacy was NOT breached, the Data Owner(s) (Responsible Officers) should send a brief summary of the investigation to the Data Protection Officer, including the reasons for concluding that personal data privacy was not breached
6. Receive Feedback	If personal data privacy was NOT breached, the Data Protection Officer should send a brief summary of the investigation to the reporting party, including the reasons for concluding that personal data privacy was not breached.

Step	Description
	The Group Executive Committee and District Commissioner should also be informed.

7. Statutory Notification	If personal data privacy WAS breached, the impact of the breach should be determined by the Data Protection Officer. If the Data Protection Officer determines that the rights and freedoms of the data subject have been infringed it is likely that the breach should be reported.
	
	If it is considered that the breach is not reportable to the ICO, the reason for this conclusion must be logged.
	
	If the breach is reportable (via https://ico.org.uk/for-organisations/report-a-breach/) it should be reported to the ICO within 72 hours where feasible. If this is not feasible, the reasons for the delay should also be reported.
	
	The following information should be reported to the ICO:
	
	• A description of the nature of the personal data breach including, where possible:
	  ○ The categories and approximate number of individuals concerned; and
	  ○ The categories and approximate number of personal data records concerned;
	• The name and contact details of the Data Protection Officer or other contact point where more information can be obtained;
	• A description of the likely consequences of the personal data breach;
	• A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects
	
	Where this information is not fully available, reporting may be completed in phases with a minimal delay.
	
	Evidence of notification, including time and date of notification, should be retained in all cases.

8. Receive Confirmation	If personal data privacy WAS breached, the Data Protection Officer should send a brief summary to the reporting party, confirming that the matter is being treated as a data privacy breach. The Group Executive Committee and District Commissioner should also be informed.
9. Receive Notification	If personal data privacy WAS breached and the breach is considered of sufficiently high risk to the rights and freedoms of the individual such that they may need to take steps to further protect themselves (e.g. loss of financial, health or confidential contact details, or where safety or safeguarding is at risk) the data subject(s) must be advised. Such notification should include: • The name and contact details of our Data Protection Officer or other contact point where more information can be obtained; • A description of the likely consequences of the personal data breach

Step	Description
	• A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects. Evidence of notification, including time and date of notification, should be retained in all cases
10. Receive Notification	The ICO should acknowledge receipt of any data breach notification and a record of receipt should be retained with time and date evidence.
11. Corrective / Preventative Measures	If personal data privacy WAS breached, in additional to any immediate action taken a full root cause analysis should be conducted. Corrective actions should be taken to secure any further personal data breaches. Based upon the root cause analysis, preventative measures may be taken to prevent or minimise the likelihood or the same or any similar reoccurrences.

Annex 1 – General Data Privacy Impact Assessment

1st Howden-le-Wear Scout Group has determined the need for a Data Privacy Impact Assessment (PIA).
This is because 1st Howden-le-Wear Scout Group:

– 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

1st Howden-le-Wear Scout Group 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	Financial penalties Other enforcement actions Reputational risk

Data breach	Data confidentiality	Rules of the Scout Association	
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 1st Howden-le-Wear Scout Group Data Protection and Privacy Policy.

Annex 2 – Refusal or charging for requests

In all cases the request must relate to the individual (Data Subject) making the request or to a child/ward of the person making the request.

Where the 1st Howden-le-Wear Scout Group is known to hold no data about a data subject, this should clearly be communicated upon request.

Where data subjects request to know what type of data is held about them, this should be considered as a subject access request of limited scope.

Data Subject Access Requests

The 1st Howden-le-Wear Scout Group will not respond to **access requests** which are considered unfounded (including malicious requests which are considered, based on prior evidence, as intended solely to inconvenience 1st Howden-le-Wear Scout Group) or which are repetitive.

Data Subject Correction Requests

The 1st Howden-le-Wear Scout Group may choose not to **correct subject data** where the 1st Howden-le-Wear Scout Group considers that the data held is correct, where changing the data breaches other overriding regulatory requirements (including the rights or freedoms or other natural persons) or where the request is considered malicious (minor corrections which are considered, basis on prior evidence, as intended solely to inconvenience 1st Howden-le-Wear Scout Group).

Data Subject Deletion Requests

Note that the right to request data deletion ('right to be forgotten') is not absolute and applies when:

– The personal data is no longer necessary in relation to the purpose for which it was originally collected/processed (i.e. the data retention period defined in the Data Protection Policy has elapsed)

– The individual withdraws consent (e.g. terminates their membership)

– The individual objects to the processing and there is no overriding legitimate interest for continuing the processing (including storage)

– The personal data was unlawfully processed (i.e. otherwise in breach of the UK Data Protection Act).

– The personal data has to be erased in order to comply with a legal obligation.

Note that because children may not have been able to fully appreciate the risks of providing consent while a minor, additional consideration should be given to requests to delete data when the data relates to a young person, regardless of their age at the time of the deletion request.

The 1st Howden-le-Wear Scout Group may choose not to delete the data for the following reasons:

– To exercise the right of freedom of expression and information (e.g. data contained in a 1st Howden-le-Wear Scout Group

newsletter, blog etc)

– To comply with a legal obligation for the performance of a public interest task or exercise of official authority (e.g. to retain safeguarding or safety data)

– For public health purposes in the public interest (e.g. medical records relating to an outbreak of illness on camps)

– Archiving purposes in the public interest, scientific research historical research or statistical purposes (e.g. data of historical significance to local or national scouting)

– The exercise or defence of legal claims (e.g. complaints data, employment records, financial records etc)

Charging

In considering that 1st Howden-le-Wear Scout Group is a not for profit charity, the 1st Howden-le-Wear Scout Group reserves the right to charge a reasonable fee (based upon a volunteer rate of £14.00/hr) for data subject access requests which are considered excessive by way of the volume of data to be searched or the volume of data to be redacted and which exceed 40 hours of volunteer time. It is very unlikely a charge will need to be made and no charge will be made for correction or deletion request.

Informing the Data Subject of a refusal or potential charges

Where requests are refused, the 1st Howden-le-Wear Scout Group Secretary must advise the data subject of the reason why the request will not be complied with and the data subjects right to complaint to the ICO and to seek judicial remedy.

Where a charge is proposed the data subject must be informed.

Annex 3 – Complex Data Requests

1st Howden-le-Wear Scout Group considers the following data subject access 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 as soon as possible, and always within 90 days of receiving the request.

– Any request involving a combination of electronic and hard copy data

– Any request involving multiple data stores from within the 1st Howden-le-Wear Scout Group Office 365 environment (e.g. email accounts, OneDrive folders, SharePoint sites [lists, folders, databases])

– Any request involving a 1st Howden-le-Wear Scout Group Office 365 data store and any other system (e.g. Compass membership database etc)

– Any request involving data held by 1st Howden-le-Wear Scout Group volunteers in personal (secure) storage locations

– All other such requests are considered simple and the data should be provided to the data subject 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 1st Howden-le-Wear Scout Group to access, redact and provide data, will provide a definitive determination of whether a data subject access request is considered simple or complex.