General Data Protection Regulations and IT Systems Acceptable Use Policies and Procedures

Elements updated in May 2020

Scouts
Merseyside

merseysidescouts.com
#SkillsForLife

Policy Contents

Data Protection Policy
for Merseyside Scouts

Issue 3: May 2020

About this policy

This Data Protection policy applies to all operations of Merseyside County Scout Council, including those at Tawd Vale Camp Site. It does not cover the operations of Districts and Groups, who should have their own policy.

The policy is designed to ensure that Merseyside County Scout Council complies with its obligations under the Data Protection Act (to be replaced with the General Data Protection Regulation (GDPR) in 2018) and conforms to the following eight data protection principles:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
    a. at least one of the conditions in Schedule 2 is met, and
    b. in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The County Secretary is the owner of this policy and responsible for its regular review (at least yearly) and update as necessary. The County will appoint a Data Protection Officer, and Data Controller, under GDPR.

The personal data we hold

Data description	Personal data included	Stored using	Retention policy	Responsible officer
Information about our adult members	Contact information, appointments, training records, activity permits and awards. (Includes sensitive data, as defined)	For adult members - Compass membership management system, provided by UK Scout Association	Retained whilst a current member. A subset of data is retained when a membership ceases in order to support the vetting policy should the person reapply	County Appoint ments Secretary / DPO

			for membership	
Information about Safeguarding incidents	Contact information and information regarding the nature of any allegation, the status and outcome of the investigation	Paper, Office 365 Email and Electronic Files (including SharePoint)	Indefinitely	County Commissioner
Information about our employees	Applications of jobs where candidate is unsuccessful	Office 365 Email	6 months after notifying candidate	County Commissioner
	Contact details, start dates, annual leave, TOIL, contract, references, copy of other relevant documentation (e.g. disciplinary letters) (Includes sensitive data, as defined)	SharePoint	5 years following the employee leaving employment	County Commissioner
	Contact details, salary and pension contribution information	Paper, secured in County Office and Office 365 Email	Indefinitely	County Commissioner
	Payroll information, including salary and other allowances, P60, P45, P11D and P6 notices.	Paper, secured in County Office and Office 365 Email	7 years	County Treasurer
Information about accidents and near misses	Contact details and nature of accident	Paper form stored in Tawd Vale Site Office	3 years after end of investigation	ACC Tawd Vale
Information about our event attendees	Name and address of group leader, name, DOB, special diet and T-Shirt size of each participant	Paper records and Eventbrite	2 years from end of event. Aggregated summary statistics indefinitely.	Relevant ACC
	Name and address of group leader, name, DOB, special diet and medical condition of each participant	Paper records and Eventbrite	2 years from end of event. Aggregated summary statistics indefinitely.	Relevant ACC

	Contact details, next of kin information, medical conditions and special diets. (Includes sensitive data, as defined)	Paper records and Eventbrite	Destroyed after event, unless medical incident and then kept for 3 years.	Relevant ACC
Information about general enquirers	Contact information and nature of enquiry, which may contain personal data	County email system	Indefinitely	County Administ-rators
Information about complainants	Contact information and nature of complaint, which may contain personal data	County email system	Indefinitely	County Commissioner
Information about our customers	Contact information	Paper forms stored in filing cabinet and SharePoint	5 years after booking occurs	ACC Tawd Vale
Information about people registered to our mailing lists	Contact information	Mailchimp (3rd party system)	Indefinitely, unless the individual requests removal	County Commissioner
Information captured via the Tawd Vale CCTV system	CCTV footage	Unify on site storage, with cloud access to approved users (see IT AUP)	Over-written every c.30 days	County Commissioner

For completeness, we also hold the following information which is not categorised as Personal Data but has the following retention policies applied:

Data description	**Retention policy**	**Responsible officer**
Finance – purchase ledgers, record of payments made, invoices, bank paying in counterfoils, bank statements, remittance advices, correspondence regarding donations, bank reconciliation.	Indefinitely	County Treasurer
Finance – Receipt cash book and sales ledger	Indefinitely	County Treasurer
Finance - Fixed assets register	Indefinitely	County Treasurer
Finance - Deed of covenant/Gift aid declaration and legacies	Indefinitely	County Treasurer
Buildings – Deeds of title	Indefinitely	County Treasurer

Buildings – Leases	Indefinitely	County Treasurer
Buildings – Documentation regarding plant and machinery	Indefinitely	County Treasurer
Buildings – records of major refurbishments, warranties, planning consent, health & safety files.	Indefinitely	County Treasurer
Trustee's minutes	Indefinitely	County Secretary
Annual accounts and annual reports	Indefinitely	County Secretary
Investment and insurance policy records	Indefinitely	County Treasurer
Insurance policies	Indefinitely	County Secretary
Employer's Liability insurance certificate	Indefinitely	County Secretary
Health and safety records	Indefinitely	County Secretary
Contract with customers, suppliers or agents, licensing agreements, rental/ hire purchase agreements, indemnities and guarantees and other agreements or contracts	Indefinitely	County Secretary

Our security policies

The following security policies will apply to the storing of personal data as outlined in this policy. These security policies are mandatory.

Overarching policies

- **Need to know** – We only give people access to the data that they need to carry out their role. If people change roles, we review access accordingly.
- **Passwords** – We use systems that force complex password complexity. Changed regularly or set once and keep until you think the password has been compromised.
- **Commercially available software** – where possible we use third party software to store personal data (provided as software-as-a-service), where the software is regularly testing and patched for security vulnerabilities.
- **Employment** – We ensure our employees are made aware of their data protection obligations
- **Transporting data** – We only transport data using physical media if absolutely necessary and then using encrypted media only.
- **We keep people informed** – we tell people why we are collecting their data and how we use it, at the point in time we collect it.

Physical storage

- **Limiting storage** – We limit the amount of personal data we physical store to the absolute minimum. Only those with a need to know will have access to the data.
- **Locked** – Physical documents with personal data will be store in a locked cabinet.

IT network

- **Acceptable use** – Our IT Acceptable Use Policy outlines how we should use the charity's IT systems.
- **Boundary security** – Our IT network at the Tea Factory and at Tawd Vale shall have a boundary firewall which restricts inbound access to those ports and protocols specifically approved, which is maintained and supported.
- **Internet filtering** – All internet traffic (including public Wi-Fi) shall be filtered to ensure that inappropriate websites cannot be accessed
- **IT Security patching** – The latest available IT Security patches are installed regularly and automatically.
- **Virus** – A virus scanning service is installed on all devices and regularly monitored.
- **File storage** – documents containing personal data should only be stored in an appropriate document library on the County's SharePoint site, and not on the personal devices of volunteers or charity provided devices.
- **Encryption** – All devices are disk encrypted.

Email

- **Acceptable use** – Our IT Acceptable Use Policy outlines how we should use the charity's email system.
- **Restriction** - Our volunteers and staff should use the Office 365 email system as their primary method for receiving, storing and sending of emails, and always when they are transmitting personal data.
- **Virus, Malware and Phishing protection** – All emails will be scanned for virus, malware and phishing.
- **IT security** - We rely upon the IT security provisions of Office 365 to provide an adequate level of security for our needs.

Volunteer equipment

- **Virus** – A virus scanning service must be installed on all devices and regularly checked.
- **Encryption** – All devices are disk encrypted with disk encryption, such as Bitlocker.
- **Removable storage** – Removable devices that will contain personal data should be encrypted using Bitlocker or similar encryption.

Third parties

- **Third party processing** – Other than The Scout Association, we limit the use of third parties to process personal data collected by Merseyside County Scout Council and only do so where we have the express permission of the County Commissioner.
- **Third party compliance** – We ensure third parties we contract with to store personal data comply with the principles of this policy, have an information security policy in place and ideally hold an information security standard (such as ISO 27001).
- **Limiting exports** – When exporting data from third party systems (e.g. Compass), we only export the data we need for the purpose we need it for and destroy if immediately after it has been used for that purpose
- **Google Docs (including Google Forms)** – We do not use Google Docs or Forms for the collation of personal information due to the data and forms collected being stored on users personal storage. If we need to use this functionality, we use Microsoft Forms (as part of our Office365 offering).

Consent

Where we do not have a lawful basis to hold or process data, we will seek the express consent of individuals to hold data about them. This will be by specific and unambiguous statements that must be opted-into on any forms (electronic or otherwise) and systems. In some circumstances due to the organisation of the Scouts, we ask our members to ensure they have express consent for the data they are submitting to us.

An example for an event we are organising:

> *"I consent to my name, date of birth, t-shirt size and information about my special diet to be used for the purposes of administering the event by ensuring that the correct security wristband is assigned, t- shirt ordered and meal options provided. We will not use this data for any other purpose than this event, except in aggregate to provide statistics for historical reference. We will delete this data one year after the event ends."*

Data Subject Access Requests

Should a member of Merseyside Scouts or a member of the public request a copy of any personal information which Merseyside County Scout Council holds, then the following process should be followed:

1. The individual should write to the County Office outlining the personal data they are seeking to obtain who will refer to the Data Protection Officer.
2. The Data Protection Officer shall acknowledge the request by email.
3. The Data Protection Officer shall seek to verify the identity of the individual and that they are lawfully entitled to request a copy of the personal data. This may involve asking for information such as a membership number, date of birth, address, or documentary evidence.
4. The Data Protection Officer will collate the data requested, noting that we cannot provide data held by other organisations such as the Scout Association, Districts or Groups. The data should be carefully analysed to ensure it does not refer to any other individuals, in which case it should be redacted.
5. Within 30 days of the receiving the request, the Data Protection Officer will provide the data to the individual. This will normally be by email.
6. There will be a charge of £10.

For more information about our legal obligations, refer to the ICO website.

Right to erasure (Right to be forgotten)

Should a member of Merseyside Scouts or a member of the public wish for their personal information to be erased, then the following process should be followed:

- The individual should write to the County Secretary outlining the personal data they are seeking to erase.
- The County Secretary shall consult the County Chair, County Commissioner and DPO, to make a decision as to whether the request should be processed. Guidance from the ICO should be followed. Whilst Merseyside Scouts will not seek to refuse the request unreasonably, it has a number of statutory obligations to comply with and uses personal data as part of its vetting and safeguarding procedures.
- If it is deemed that the data shall be deleted, then the County Secretary will confirm to the individual the timescales involved and instruct the necessary responsible officer to delete it.

Correcting inaccurate personal data

Should a member of Merseyside Scouts or a member of the public believe that information that we hold about them is inaccurate, they should write to the County Secretary outlining the inaccuracy. The County Secretary will then seek to correct the data and confirm back to the individual.

Reporting a breach

A breach is defined as any event which “leads to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data”. If a breach occurs, the County Secretary should be immediately informed.

The County Secretary (in consultation with the County Chair, County Commissioner and DPO) will need to consider if the breach is likely to “result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage”. If it does, the ICO should be informed within 72 hours of the breach occurring.

If the breach results in a high risk to the rights of the individuals involved, they should also be informed directly.

Data Privacy Management Procedure for Merseyside Scouts

Issue 2: August 2018

About this procedure

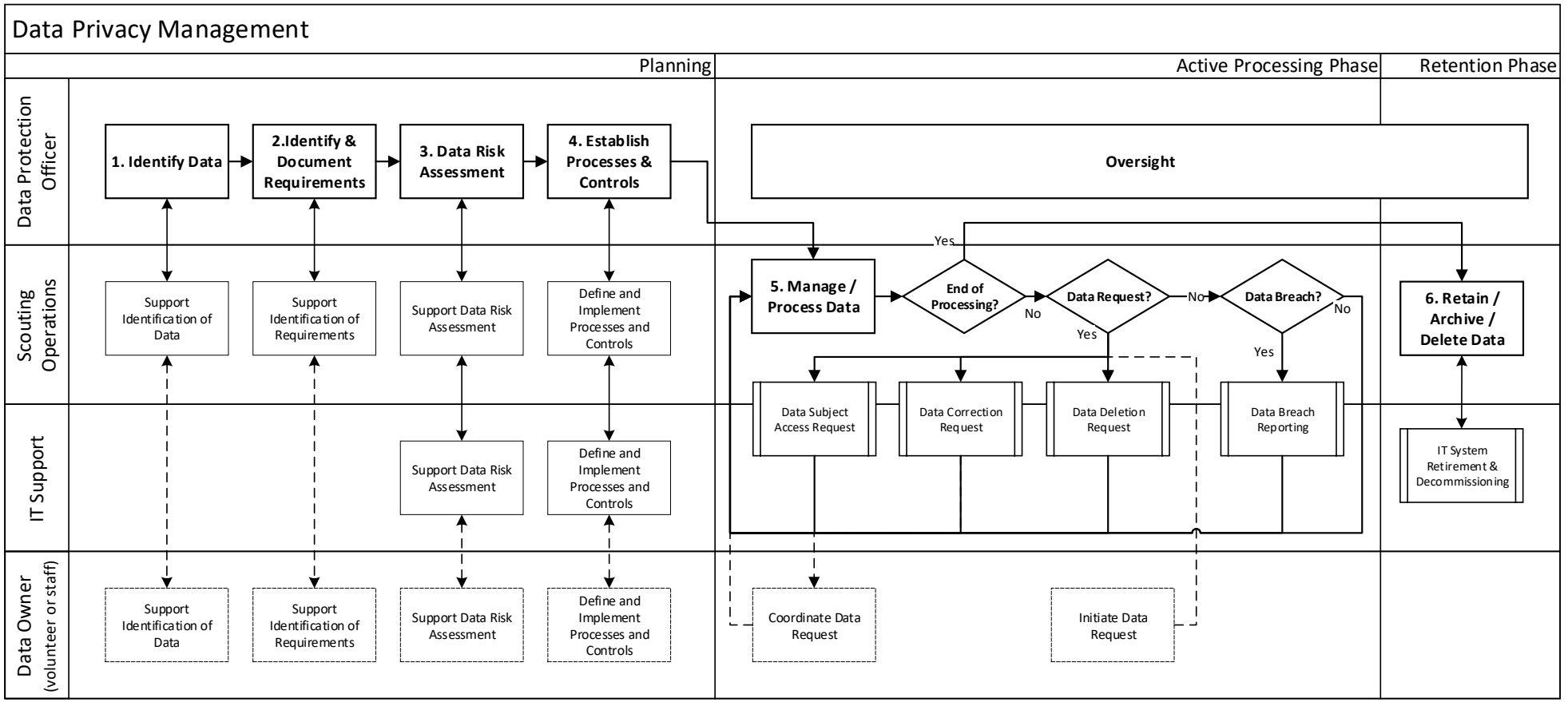
This procedure defines how Merseyside County Scout Council will manage personal data to assure appropriate data privacy in accordance with the UK Data Protection Bill 2017. It should be read in conjunction with current information and guidance published by the UK Information Commissioner's Office (ICO – 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 members, staff, suppliers, customers etc. As Merseyside County Scout Council 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 county 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 or members of staff. For each set of personal data processed, the county 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 or members of staff. 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), other appropriate volunteers or members of staff including the county IT Administrator. 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. Merseyside County Scout Council 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 county 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 county 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) • Processing for purposes of scientific/historical research and statistics. In these cases, processing must cease unless the scout county 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 the County'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 county 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 scout county; • 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 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 county data retention policy

Annex 1 – General Data Privacy Impact Assessment

Merseyside County Scout Council has determined the need for a Data Privacy Impact Assessment (PIA). This is because the scout county:

- 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

Merseyside County Scout Council 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 county data protection policy.

Annex 2 – Complex Data Portability Requests

Merseyside County Scout Council 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 county Office 365 environment (e.g. email accounts, OneDrive folders, SharePoint sites [lists, folders, databases])
- Any request involving a county Office 365 data store and any other system (e.g. MailChimp, Eventbrite, Compass membership database etc)
- Any request involving data held by county 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 county to transfer the data, will provide a definitive determination of whether a data transfer request is considered simple or complex.

Data Subject Access Request Procedure for Merseyside Scouts

Issue 2: August 2018

About this procedure

This procedure defines how Merseyside County Scout Council will manage data subject access requests 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 members, staff, suppliers, customers etc. As Merseyside County Scout Council 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 county Data Protection Policy.

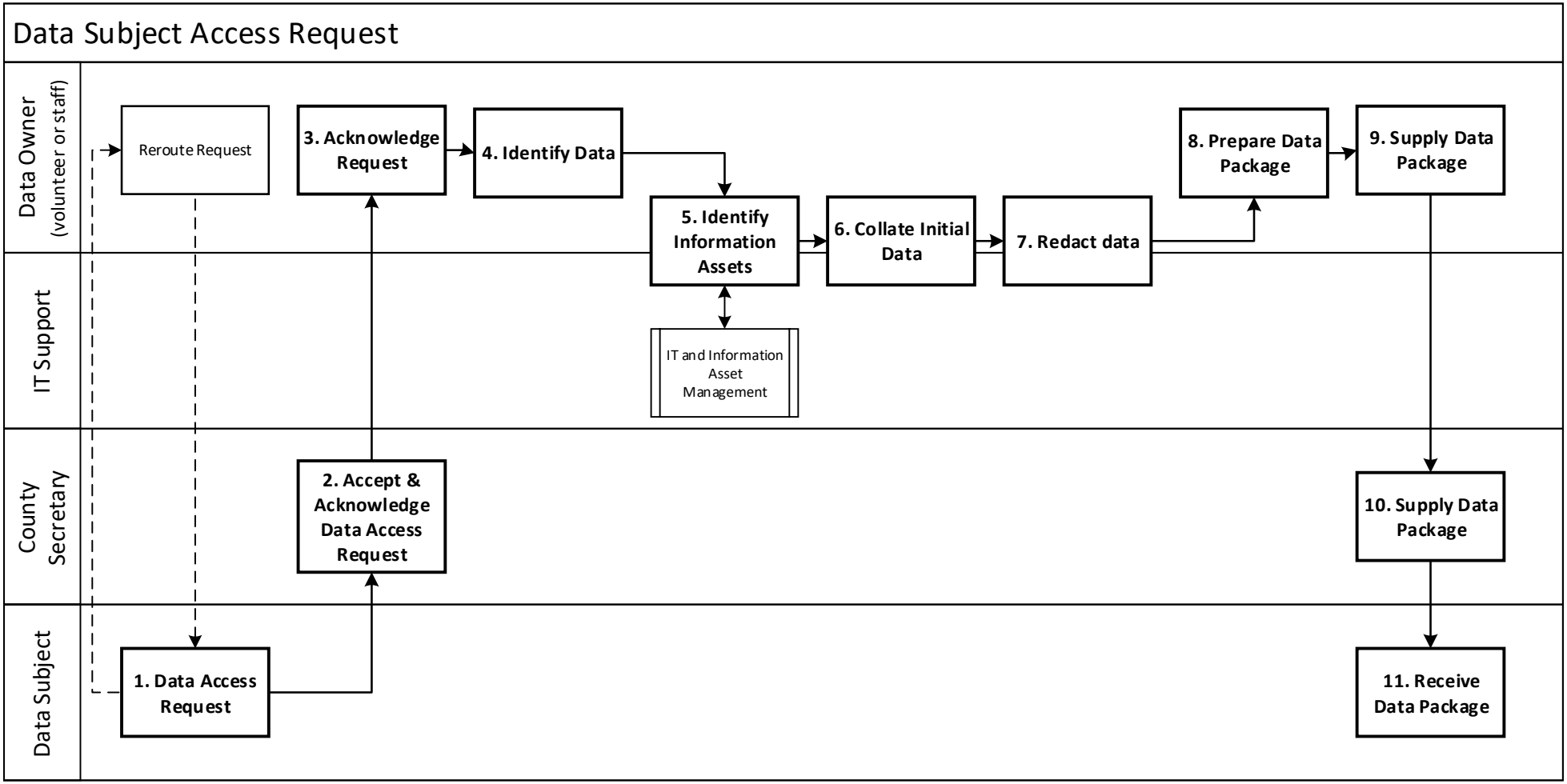
Where the county is known to hold no data about a data subject, this should clearly be communicated upon request.

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.

The scout county will not respond to data subject access requests which are considered unfounded (including malicious requests which are considered, basis on prior evidence, as intended solely to inconvenience the organisation, staff or volunteers) or which are repetitive. Where such requests are refused, the County DPO 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.

In considering that Merseyside County Scout Council is a not for profit charity, the scout county reserves the right to charge a reasonable fee (based upon a volunteer rate of £14.00/hr or the applicable staff costs) 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 staff or volunteer time.

The general process for implementing data subject access requests is shown overleaf.



This process is described in more detail below – for the purpose of this process, the Data Protection Officer will act in place of the County Secretary where the County Secretary is not also the Data Protection Officer.

Step	Description
1. Data Access Request	The Data Subject makes a data subject access request. This should be directed to the County Secretary (any member of staff of any other volunteer, including the data owner (Responsible Officer) should direct the request to the County Office.
2. Accept and Acknowledge Data Access request	The County Office will refer the request to the DPO who should immediately acknowledge receipt of the data subject access request. The DPO should maintain a log of all requests including: • Date request received • Data subject name and contact details • Scope of data subject access 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 DPO may refuse or charge for a request as outlined above. Where the scope of the request is not specific, the DPO should seek to clarify the scope of the request i.e. whether it relates to all data held by the scout county, or to a specific subset of data (specific datasets, timescales, relating to specific events etc) The DPO should determine whether the data subject access request is complex or simple. If the request is considered complex (see Annex 1), the DPO 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 1), the DPO should inform the data subject that the requested data will be provided within 1 month. The DPO should inform the data owner(s) (Responsible officers) of the data subject access request.
3. Acknowledge Request	The data owner(s) (Responsible Officers) should acknowledge the request to the DPO and prioritise their activities accordioning
4. Identify Data	Based upon the defined scope of the data subject access 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 access request, and the datasets identified by the data owner(s) (Responsible Officers), the data owner(s) and county IT Administrator 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, MailChimp, Evenntbrite)
6. Collate Initial Data	Using appropriate search criteria (filters, date ranges, keywords etc) derived from the scope of the data subject access request, the data owner(s) (Responsible Officers) and county IT Administrator 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 county IT Administrator will 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)

Step	Description
	• Any data which does not directly relate to the scope of the data access 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 Data Package	The data owner(s) (Responsible Officers) should prepare the necessary data 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 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 County 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 county account and User ID).
10. Supply Data Package	The DPO 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.

Annex 1 – Complex Data Subject Access Requests

Merseyside County Scout Council 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 data held in the county archives
- Any request involving a combination of electronic and hard copy data
- Any request involving multiple data stores from within the county Office 365 environment (e.g. email accounts, OneDrive folders, SharePoint sites [lists, folders, databases])
- Any request involving a county Office 365 data store and any other system (e.g. MailChimp, Eventbrite, Compass membership database etc)
- Any request involving data held by county 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 county to access, redact and provide data, will provide a definitive determination of whether a data subject access request is considered simple or complex.

Data Subject Correction Request Procedure for Merseyside Scouts

Issue 2: August 2018

About this procedure

This procedure defines how Merseyside County Scout Council will manage data subject requests to correct (rectify) erroneous or incomplete data 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/)

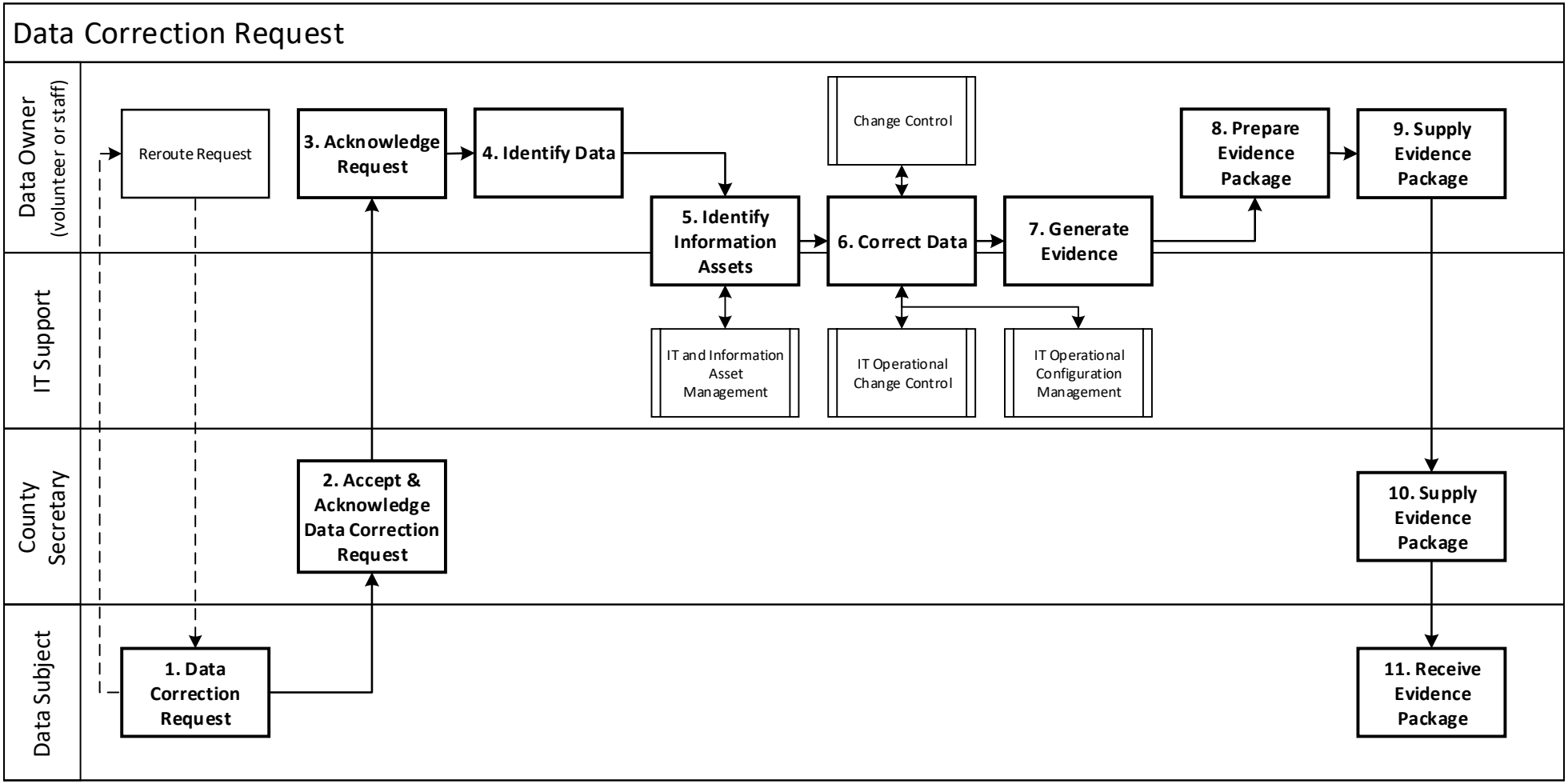
Note that once the UK leaves the European Union, additional requirements of the European Union General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) may continue to apply with respect to data processed relating to EU citizens, which may include members, staff, suppliers, customers etc. As Merseyside County Scout Council 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 county Data Protection Policy.

Where possible, corrections to personal data should be made by county staff or volunteer administrators using standard data management processes and without recourse to this procedure.

The scout county may choose not to correct subject data where the scout county 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 the organisation, staff or volunteers). Where such requests are refused, the County 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.

The general process for implementing data subject correction requests is shown overleaf. Note that depending upon the scope of the request, this process may be combined with a data deletion request.



This process is described in more detail below – for the purpose of this process, the Data Protection Officer will act in place of the County Secretary where the County Secretary is not also the Data Protection Officer.

Step	Description
1. Data Correction Request	The Data Subject makes a data subject access request. This should be directed to the County Secretary (any member of staff of any other volunteer, including the data owner (Responsible Officer) should direct the request to the County Office.
2. Accept and Acknowledge Data Correction request	The County Office will refer the request to the DPO who should immediately acknowledge receipt of the request. The DPO should maintain a log of all requests including: • Date request received • Data subject name and contact details • Scope of data correction request • Date of request acknowledgement • Date data or data access to be corrected This list may be consulted to determine whether a request is repetitious or malicious. The DPO may refuse or charge for a request as outlined above. Where the scope of the request is not specific, the DPO should seek to clarify the scope of the request i.e. whether it relates to all data held by the scout county, or to a specific subset of data (specific datasets, timescales, relating to specific events etc) The DPO should determine whether the data correction request is complex or simple. If the request is considered complex (see Annex 1), the DPO should inform the data subject that the request is complex and that the requested correction will be made within 90 days. If the request is not considered complex (see Annex 1), the DPO should inform the data subject that the data correction will be made within 1 month. The DPO should inform the data owner(s) (Responsible officers) of the data correction request.
3. Acknowledge Request	The data owner(s) (Responsible Officers) should acknowledge the request to the DPO and prioritise their activities accordioning
4. Identify Data	Based upon the defined scope of the data subject correction request, the data owner(s) (Responsible Officers) should identify the specific datasets that need to be corrected.
5. Identify Information Assets	Based upon the defined scope of the data subject correction request, and the datasets identified by the data owner(s) (Responsible Officers), the data owner(s) and county IT Administrator 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. Mailchimp, Eventbrite, Compass) Note that at this stage it may be discovered that erroneous data may have been shared with third parties. Where this is the case the third party should be requested to also correct the data and provide evidence of compliance.
6. Correct Data	Using appropriate search criteria (filters, date ranges, keywords etc) derived from the scope of the data subject correction request, the data owner(s) (Responsible Officers) and county IT Administrator will correct data and records within the scope of the request (as hard copies and/or a separate electronic copy). If there are any queries with respect to the changes to be made, these should be clarified with the data owner(s) (Responsible Officers), DPO or data subject as appropriate.

Step	Description
7. Generate Evidence	The data owner(s) (Responsible Officers), assisted by the county IT Administrator will generate and retain evidence of the data correction being made. This will typically include: • A copy of the corrected hard copy • Before and after screen shots of the corrected data Care should be taken to redact any evidence in accordance with step 7 of the data subject access request procedure to ensure that the evidence contains no personal, sensitive or confidential data.
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 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 Evidence Package	The data owner(s) (Responsible Officers) should supply the evidence package to the County 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 county account and User ID).
10. Supply Evidence Package	The DPO should supply the evidence 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 correction request log updated.
11. Receive Evidence Package	The data subject receives the evidence package (or access to the evidence package) and should acknowledge receipt. Any subsequent correction request may be reconsidered as malicious described above.

Annex 1 – Complex Data Subject Correction Requests

Merseyside County Scout Council considers the following data subject correction 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 evidence should be provided to the data subject as soon as possible, and always within 90 days of receiving the request.

- Any request involving data held in the county archives
- Any request involving a combination of electronic and hard copy data
- Any request involving multiple data stores from within the county Office 365 environment (e.g. email accounts, OneDrive folders, SharePoint sites [lists, folders, databases])
- Any request involving a county Office 365 data store and any other system (e.g. MailChimp, Eventbrite, Compass membership database etc)
- Any request involving data held by county volunteers in personal (secure) storage locations

All other such requests are considered simple and the data should be corrected and evidence 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 county to correct the data, will provide a definitive determination of whether a data subject correction request is considered simple or complex.

Data Subject Deletion Request Procedure for Merseyside Scouts

Issue 2 : August 2018

About this procedure

This procedure defines how Merseyside County Scout Council will manage data subject requests to delete (erase) data ('right to be forgotten') 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 members, staff, suppliers, customers etc. As Merseyside County Scout Council 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 county Data Protection Policy.

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 (i.e. leaves the employment of the scout county or 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.
- The personal data is processed in relation to the offer of information society services to a child.

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.

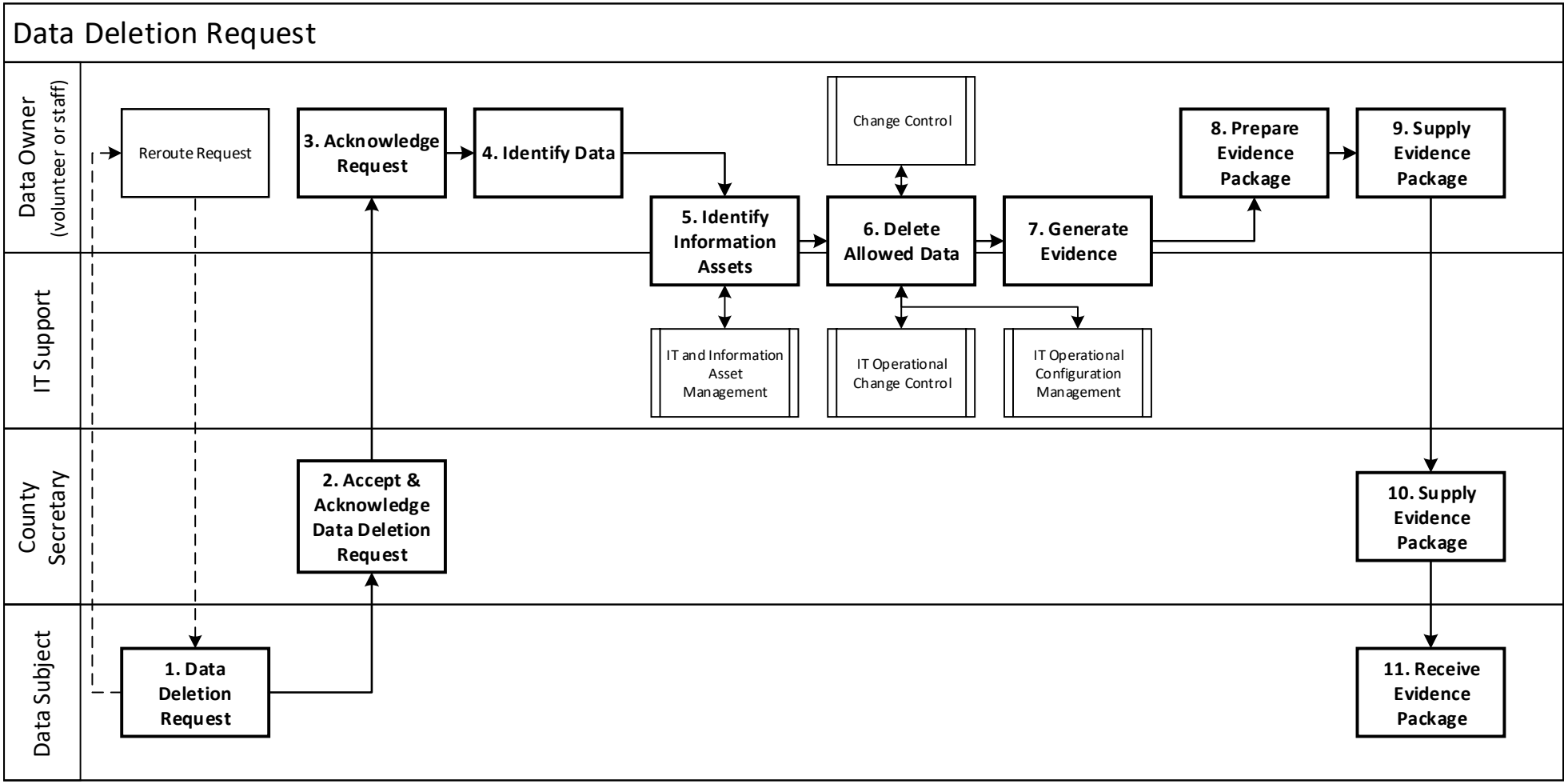
The scout county may choose not to delete the data for the following reasons:

- To exercise the right of freedom of expression and information (e.g. data contained in a county 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)

Where such requests are refused, the County Secretary must advise the data subject of the reason why the request will not be complied with.

The general process for implementing data subject correction requests is shown overleaf. Note that depending upon the scope of the request, this process may be combined with a data deletion request.



This process is described in more detail below – for the purpose of this process, the Data Protection Officer will act in place of the County Secretary where the County Secretary is not also the Data Protection Officer.

Step	Description
1. Data Deletion Request	The Data Subject makes a data subject access request. This should be directed to the County Secretary (any member of staff of any other volunteer, including the data owner (Responsible Officer) should direct the request to the County Office.
2. Accept and Acknowledge Data Deletion request	The County Office will refer the request to the DPO who should immediately acknowledge receipt of the request. The DPO should maintain a log of all requests including: • Date request received • Data subject name and contact details • Scope of data subject deletion request • Date of request acknowledgement • Date data deletion confirmed The DPO may refuse a data deletion request as outlined above. Where the scope of the request is not specific, the DPO should seek to clarify the scope of the request i.e. exactly what data should be deleted. The DPO should determine whether the data subject deletion request is complex or simple. If the request is considered complex (see Annex 1), the DPO should inform the data subject that the request is complex and that the requested data will be deleted within 90 days. If the request is not considered complex (see Annex 1), the DPO should inform the data subject that the data will be deleted within 1 month. The DPO should inform the data owner(s) (Responsible officers) of the data subject deletion request.
3. Acknowledge Request	The data owner(s) (Responsible Officers) should acknowledge the data correction deletion to the County Secretary and prioritise their activities accordingly
4. Identify Data	Based upon the defined scope of the data subject deletion request, the data owner(s) (Responsible Officers) should identify the specific datasets that need to be edited or deleted.
5. Identify Information Assets	Based upon the defined scope of the data subject deletion request, and the datasets identified by the data owner(s) (Responsible Officers), the data owner(s) and county IT Administrator 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. MailChimp, Eventbrite, Compass) Note that at this stage it may be discovered that data may have been shared with third parties (e.g. the Scout Association, Scout Districts etc). Where this is the case the third party should be requested to also delete the data and provide evidence of compliance.
6. Delete Allowed Data	Using appropriate search criteria (filters, date ranges, keywords etc) derived from the scope of the data subject correction request, the data owner(s) (Responsible Officers) and county IT Administrator will securely delete data and records within the scope of the request (as hard copies and/or a separate electronic copy). Where records contain personal data within the scope of the deletion request and other data (which may need to be retained for other purposes), consideration should be given to deleting only the personal data to pseudonymise the record.

Step	Description
	Hard copies should be shredded and disposed of as confidential waste. Electronic data should be permanently erased where possible (not just marked as deleted or moved to archive) If there are any queries with respect to the deletions to be made, these should be clarified with the data owner(s) (Responsible Officers), County Secretary or data subject as appropriate.
7. Generate Evidence	The data owner(s) (Responsible Officers), assisted by the county IT Administrator will generate and retain evidence of the data deletion being made. This will typically include: • A copy of the hard copy data that has been destroyed • A copy of the electronic data that has been deleted • Before and after screen shots of the deleted record or database Care should be taken to redact any evidence in accordance with step 7 of the data subject access request procedure to ensure that the evidence contains no personal, sensitive or confidential data.
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 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 Evidence Package	The data owner(s) (Responsible Officers) should supply the evidence package to the County 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 county account and User ID).
10. Supply Evidence Package	The DPO should supply the evidence 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 deletion request log updated.
11. Receive Evidence Package	The data subject receives the evidence package (or access to the evidence package) and should acknowledge receipt.

Annex 1 – Complex Data Subject Deletion Requests

Merseyside County Scout Council considers the following data subject correction 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 evidence should be provided to the data subject as soon as possible, and always within 90 days of receiving the request.

- Any request involving data held in the county archive
- Any request involving a combination of electronic and hard copy data
- Any request involving multiple data stores from within the county Office 365 environment (e.g. email accounts, OneDrive folders, SharePoint sites [lists, folders, databases])
- Any request involving a county Office 365 data store and any other system (e.g. Mailchimp, Eventbrite, Compass membership database etc)
- Any request involving data held by county volunteers in personal (secure) storage locations

All other such requests are considered simple and the data should be corrected and evidence 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 county to correct the data, will provide a definitive determination of whether a data subject correction request is considered simple or complex.

Data Breach Reporting Procedure for Merseyside Scouts

Issue 2: August 2018

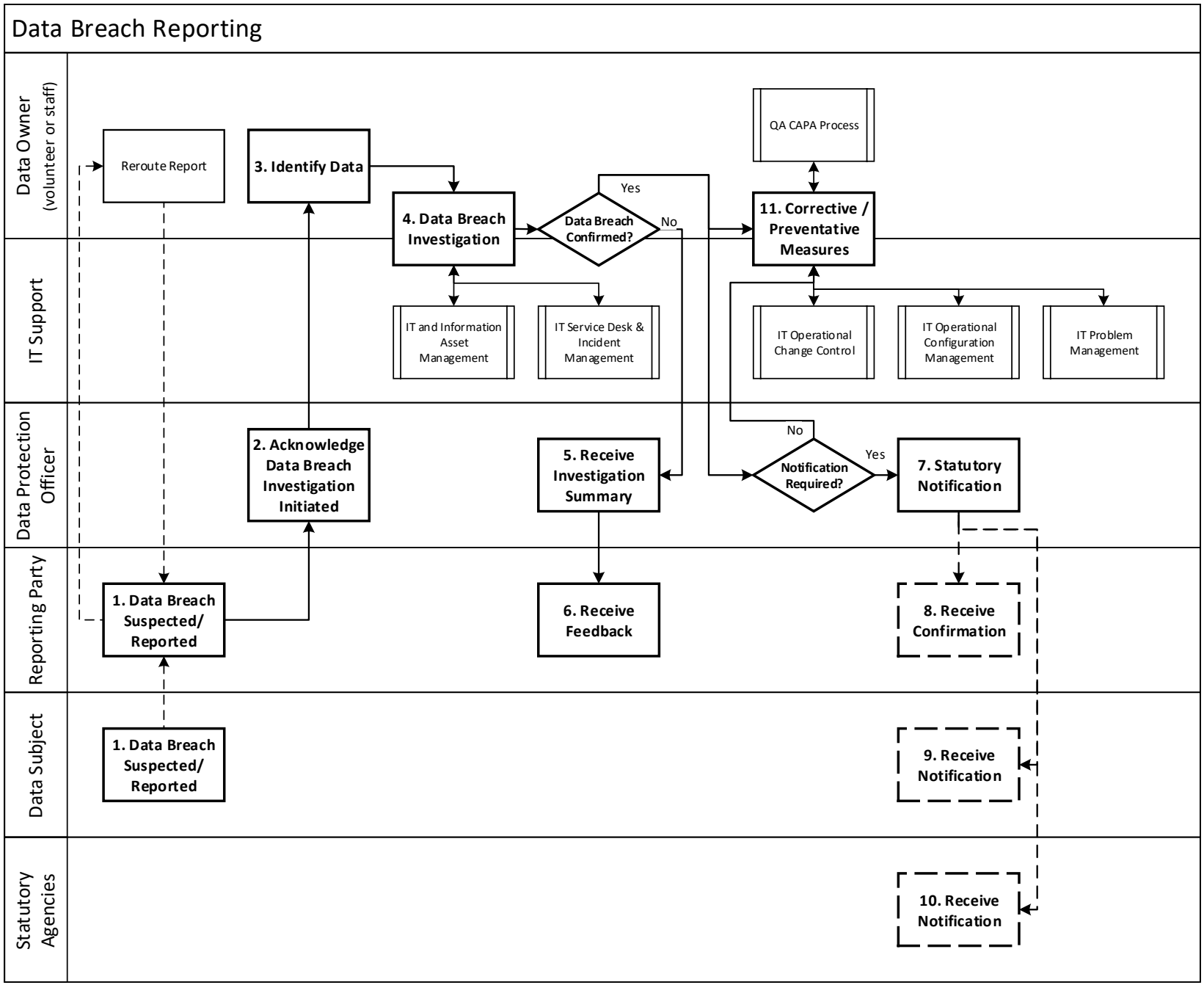
About this procedure

This procedure defines how Merseyside County Scout Council will manage personal data breaches 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 members, staff, suppliers, customers etc. As Merseyside County Scout Council 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 county Data Protection Policy.

Note that any subprocessors engaged on behalf of Merseyside County Scout Council (e.g. Microsoft, MailChimp etc) are required to report ALL data privacy breaches. They should be considered as reporting parties with respect to this procedure.


Data Breach Reporting
Data Owner (volunteer or staff)
IT Support
Data Protection Officer
Reporting Party
Data Subject
Statutory Agencies
Reroute Report
3. Identify Data
4. Data Breach Investigation
Data Breach Confirmed?
Yes
No
QA CAPA Process
11. Corrective / Preventative Measures
IT and Information Asset Management
IT Service Desk & Incident Management
IT Operational Change Control
IT Operational Configuration Management
IT Problem Management
2. Acknowledge Data Breach Investigation Initiated
5. Receive Investigation Summary
No
Notification Required?
Yes
7. Statutory Notification
1. Data Breach Suspected/ Reported
6. Receive Feedback
8. Receive Confirmation
1. Data Breach Suspected/ Reported
9. Receive Notification
10. Receive Notification

This process is described in more detail below

Step	Description
1. Data Breach Suspected / Reported	The data subject, or any other party reports a suspected or actual personal data breach. All staff and volunteers of Merseyside County Scout Council 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 other member of staff or any other volunteer receiving such a report should request the reporting party to report the matter to the Data Protection Officer and copy the Data Protection Officer will all 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 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 County Commissioner and County Chair 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 county IT Administrator will provide support to identify the IT and information assets potentially involved.
4. Data Breach Investigation	The County IT Administrator will provide support to identify the IT and information assets potentially involved. The Data Owner(s) (Responsible Officers) and the IT Administrator, assisted by other staff members or 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

Step	Description
	Where possible, immediate steps should be taken to halt or minimise the scale of the data breach. This may leverage any IT incident management procedures.
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. The County Commissioner and County Chair 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 County Commissioner and County Chair 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 in accordance with any applicable corrective and preventative action or IT problem management procedures. 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. This may involves IT change management or configuration management processes

IT Systems Acceptable Use Policy for Merseyside Scouts

Issue 3: May 2020

About this policy

This Acceptable Usage Policy covers the security and use of all Merseyside County Scout Council's IT equipment and systems. This policy applies to all Merseyside County Scout Council's employees, volunteers and partners (hereafter referred to as 'individuals').

This policy applies to all information, in whatever form, relating to Merseyside County Scout Council's charity activities, and to all information handled by Merseyside County Scout Council relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by Merseyside County Scout Council or on its behalf.

Access Control

Access to the Merseyside County Scout Council IT systems is controlled by the use of User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on Merseyside County Scout Council's IT systems.

Individuals must not:

- Allow anyone else to use their user ID/token and password on any Merseyside County Scout Council IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access Merseyside County Scout Council's IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to Merseyside County Scout Council's IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Give or transfer Merseyside County Scout Council data or software to any person or organisation outside Merseyside County Scout Council without the authority of Merseyside County Scout Council.

Internet and Email Conditions of Use

Use of Merseyside County Scout Council internet and email is intended for charity use. All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which Merseyside County Scout Council considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Send unprotected sensitive or confidential information externally.
- Forward Merseyside County Scout Council mail to personal email accounts (for example a personal Hotmail account).
- Make official or contractual commitments through the internet or email on behalf of Merseyside County Scout Council unless authorised to do so.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.

Software

Staff and volunteers must use only software that is authorised by Merseyside County Scout Council on Merseyside County Scout Council's computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on Merseyside County Scout Council computers must be approved and installed by the County Commissioner (or designate).

Monitoring and Filtering

All data that is created and stored on Merseyside County Scout Council computers and/or Internet and Email systems is the property of Merseyside County Scout Council and there is no official provision for individual data privacy.

IT system logging is in place where appropriate, and any necessary investigations may be commenced where reasonable suspicion exists of a breach of this or any other policy. Merseyside County Scout Council has the right to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be authorised by the County Commissioner (or designate), and carried out in accordance with audited, controlled internal processes and the UK Data Protection Act 1998.

This policy should be read in conjunction with our GDPR policies and procedures

Policy Implementation

This policy will be issued to all users of Merseyside County Scout Council's IT Equipment and Systems. Thereafter, use of Merseyside County Scout Council's IT Equipment and Systems will be considered as acceptance of this policy.

IT Equipment and System Administration

The table below identifies those with System Administration access to IT Equipment and Systems, at the time of the date of this policy.

Role	**Network Infrastructure**	**IT Equipment**	**VOIP Phone System**	**Office 365**	**Website and Associated Services**	**Social Media Accounts**	**Tawd Vale CCTV System**
County Commissioner	✓	✓	✓	✓	✓	✓	✓
Digital Services Manager	✓	✓	✓	✓	✓	✓	✓
Digital Engagement Manager					✓	✓	
Website Co-Ordinator					✓		
IT Competent Person (Named Designate) Chris Rutter	✓	✓	✓	✓	✓	✓	

Note: The Tawd Vale Centre Manager, the Chair of the Tawd Vale Steering Group and the Deputy County Commissioner for Adventure will also have 'User' access to the Tawd Vale CCTV system. Data captured by this system should be treated as personal data and must be managed in accordance with our GDPR policies. Release of any footage requires the approval of the County Commissioner and/or Data Protection Officer.