Policy – GDPR (Privacy Statement)

Version 5

Includes:

Data Subject Deletion Request Procedure
Data Subject Correction Request Procedure
Data Subject Access Request Procedure
Data Privacy Management Procedure
Data Privacy Management Procedure
Data Breach Reporting Procedure

Version Control				
Version	**Date**	**Content**	**Manager Approved**	**Board Approved**
V1	May 2018	New Policy	A Jones	M Howlett
V2	July 2023	General review, minor updates to reflect operating practice	A Jones	M Howlett
V3	Aug 2024	Full review	A Jones	M Howlett
V4	July 2025	Full review	G Phillips	M Howlett
V5	August 2026	Format Change	G Phillips	M Howlett

Privacy Policy

Cheshire Young Carers has created this policy which covers how we collect, use, disclose, transfer and store your data. Our full Privacy Policy is available on our website at all times and is subject to change.

General Terms

Our commitment to protecting your privacy is paramount at Cheshire Young Carers. The following statements describe how Cheshire Young Carers collects, uses and protects information. This Policy relates to our use of any personal information we collect from you or you provide to us via our website, email, SMS, phone, in letters and other correspondence and in person.

In order to provide our services, we need to handle data, this privacy statement sets out the following:

• what information Cheshire Young Carers may collect about you;

• how Cheshire Young Carers will use information we collect about you;

• when Cheshire Young Carers may use your details to contact you;

• whether Cheshire Young Carers will disclose your details to anyone else including our legal obligations;

• your rights and choices regarding the personal information you provide to us.

If you have any queries about information contained within this statement please contact us at Northern Lights Business Park, Rossfield Road, Ellesmere Port, CH65 3AW or by email: info@cheshireyoungcarers.com

What information do we collect about you?

We will collect personal information from you when you enquire about our activities, register with us, make a referral, register for specific activities, make a donation to us or otherwise provide us with personal information. We may also receive information about you from other people, for example, if a third-party service, friend or colleague refers you to our website or services.

The information we collect depends on our relationship with you and can include various categories of data as defined under the GDPR, this data typically includes name, address, additional contact details and further information you provide to us by way of registration or referral.

Full, comprehensive details regarding how we protect your information can be found in our GDPR Policy.

How do we use personal data?

We need to know your personal data to provide you with our services that you request, keep in touch with you if we have your consent to do so and to ensure our legal safeguarding obligations are met.

We will not collect any personal data from you that we do not need to provide and oversee these services.

Special Category Data

The UK GDPR singles out some types of personal data as likely to be more sensitive, and gives them extra protection:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**

Cheshire Young Carers recognises the additional sensitivy regarding the aforementioned data and this is protected further by using permission-based access within the records we hold for staff, dependent on roles.

Supporters/sponsors/donors:

We record the data you provide to us in an appropriate and safe manner in line with our Data Protection Policy. We record and keep the data about any donations we receive as per our Data Protection Policy and in line with any legal requirements set by authoritative bodies such as HMRC. We may use this data in our newsletters, website and social media, for example to express thanks for support or donations – consent for this use will be requested in advance. Under GDPR we have identified our legal basis of legitimate interest to retain information and contact you in response to your support of our organisation. If you decide that you do not wish us to use your data in this way you can contact us to withdraw consent at any time at Northern Lights Business Park, Rossfield Road, Ellesmere Port, CH65 3AW or by email: info@cheshireyoungcarers.com

Service users (young carers, parents, guardians):

If a child (young carers are children aged 6 – 18) is referred to us and accesses or interacts with our services, including the trips and activities we arrange for young carers, in order to comply with our legitimate interests (running our services and protecting those who use them) we may on occasion collect special category data (e.g. health details) which are provided in circumstances where we have responsibilities in relation to safeguarding. For example, if a young carer joins us on a residential activity we will request the necessary information in order to protect that individual, our data protection policies are designed specifically to ensure that a child's rights and interests are properly considered and protected. Children who are aged 13 and under require explicit parental consent, this is collected via consent and activity forms and can be redacted, amended or renewed at any time –

typically on a annual basis. We store these details digitally and may from time to time, where necessary, share the details of parental consent with third party providers on occasions whereby we are supporting children to participate in activities with external providers.

Due to the nature of Cheshire Young Carers work it is often that we process children's personal data. Our systems and processes are designed with protecting children's personal data in mind. We are committed to complying with the data protection principles, fairness and safeguarding is central to all our processing. Often, we rely on legitimate interests as our lawful basis for processing personal data, this is so that we are able to protect children's interests and fundamental rights. We are committed to assessing the risks that come with processing data and we take the required appropriate measures to safeguard against those risks, we outline the ways in which we take extra steps to protect this information in our GDPR Policy.

On rare occasions we will be processing individuals' data in order to protect the vital interests of another individual; this will always be in the interests of safeguarding and protection of an individual. There are occasions where information including special category data, is provided by a third party (e.g. public bodies), this will always be in a way which is reasonably expected, where they are a data controller (Martin Howlett) already and we outline the ways in which we take extra steps to protect this information in our GDPR Policy.

Visitors to our website:

We will gather general information regarding the use of our website, such as which pages are visited most frequently. Only anonymous information and statistics will be used which do not identify individual visitors. This information helps us improve the services and information we offer on our website. We may use service providers to help us collect and analyse this information. Additional information regarding cookies and links on our website can be found below under "When do we share personal data?".

When do we use your information to contact you?

If you consent to us contacting you via post we will normally send you a regular newsletter, we may also write to you with details about up and coming activities we are organising and invitations for events. We may need to contact service users via post about specific activities or events they have signed up to. If you request forms/additional correspondence we may send this via post. We may write to you to respond to any queries you have raised with us or to thank you for your support and involvement with Cheshire Young Carers.

If you consent to us contacting you via email we will normally send you a round up with news about our work, upcoming events and about how to support us on a monthly basis. We may also use your email address to respond to any queries you have raised with us, since this is more cost-effective than responding by post. We may need to contact service users via email about specific activities or events they have signed up to.

If you consent to us contacting you via telephone we may use this to answer any queries you have. We may also use it to ask if you have a new address if a mailing is returned to us saying you have moved. We may need to contact service users via telephone about specific activities or events they have signed up to. We may occasionally use it to thank you for a donation.

If you consent to us contacting you via SMS we may use this to answer any queries you may have. We may use it to contact you if you or somebody you are responsible for is due to attend a session or event and details need to be communicated to you. We may need to contact service users via SMS about specific activities or events they have signed up to.

If you consent to us contacting via social media channels this will normally be with “closed groups” . We may use it to communicate to a group of parents/carers with children involved in particular activites/trips as a way of keeping all participant parents.carers updated on the activity/trip.

We will only use your personal information to provide you with the services, products or information you have requested. Exceptions to this will be in circumstances where we are required to comply with legal obligations.

You can opt out of receiving any or all materials at any time by contacting the charity at Northern Lights Business Park, Rossfield Road, Ellesmere Port, CH65 3AW or by email: info@cheshireyoungcarers.com. We may wish to discuss your decision to no longer receive contact or materials from us if this impacts the safeguarding of our service users.

When do we share personal data?

All the personal data we process is processed by our staff, we do not pass your data on to third parties unless they are required to carry out a service which will be requested and/or agreed in advance such as pre-arranged transport agreements/use of additional third-party service providers. Any further sharing of data will be in relation to our safeguarding and legal obligations and will be done so in line with existing contracts and legal structures that are in place. We sometimes use third parties in alternative circumstances, we will be explicit that this detail is required to be shared and seek consent in advance.

Cookies

‘Cookies’ are small pieces of information sent by a web server to a web browser, which enable the server to collect information from the browser. Essentially it takes the form of a small text file deposited on your computer’s hard drive.

Cheshire Young Carers reserves the right to use cookies to ensure that you can interact with our website successfully, to identify you when you visit our website and to keep track of your browsing patterns. This data is only analysed so that we can classify the use of our website. The use of cookies does not give us access to the rest of your computer or to personal information about you.

Personal Detail Protection

Information that you submit in a registration or enquiry form is digitised, encrypted and stored on a secure server. However, the transmission of information over the Internet is never 100% secure so while we try to protect your personal information, we can’t guarantee the security of any information you submit to us via our website.

We also take appropriate measures to ensure that the information we receive is kept secure, accurate and up to date and kept only for so long as is necessary for the purposes for which it is used. We hold retention policies which are contained within our GDPR Policy. All access to our secure server is restricted only to authorised staff.

Links

Our website may include links to websites run by other organisations. Cheshire Young Carers is not responsible for the privacy practices of other organisations’ websites so you should read their privacy policies carefully.

Legal Compliance

Cheshire Young Carers have an obligation to comply with UK law, work alongside local authority regulators and services and where relevant transfer data to these bodies. For example, where a child is the subject of multi-agency interventions or where there are specific concerns about the safety or wellbeing of a young carer. Cheshire Young Carers may need to disclose your information if required to do so by law or in response to a court order or, in circumstances where we think someone is at serious risk of being harmed, we may contact the police or a local authority safeguarding team.

Your rights

You have the right to ask for a copy of the information we hold about you and to have any inaccuracies in your information corrected.

If you wish to exercise these rights, please contact us Northern Lights Business Park, Rossfield Road, Ellesmere Port, CH65 3AW or by email: info@cheshireyoungcarers.com. We are legally obliged to answer your request within 30 days but we will normally do so sooner.

Cheshire Young Carers reserves the right to amend this privacy statement. The most up to date version will be always be available on our website so please check from time to time.

Data Subject Deletion Request Procedure

About this procedure

This procedure defines how Cheshire Young Carers will manage data subject requests to delete (erase) data ('right to be forgotten'). 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 now the UK has left 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. Cheshire Young Carers does not regularly process data relating to citizens of the EU as a matter of course, it is considered that this 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 GDPR 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 relevant Policy (e.g. Data Protection or GDPR) has elapsed)
- The individual withdraws consent (i.e. leaves the employment)
- 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 must be erased to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

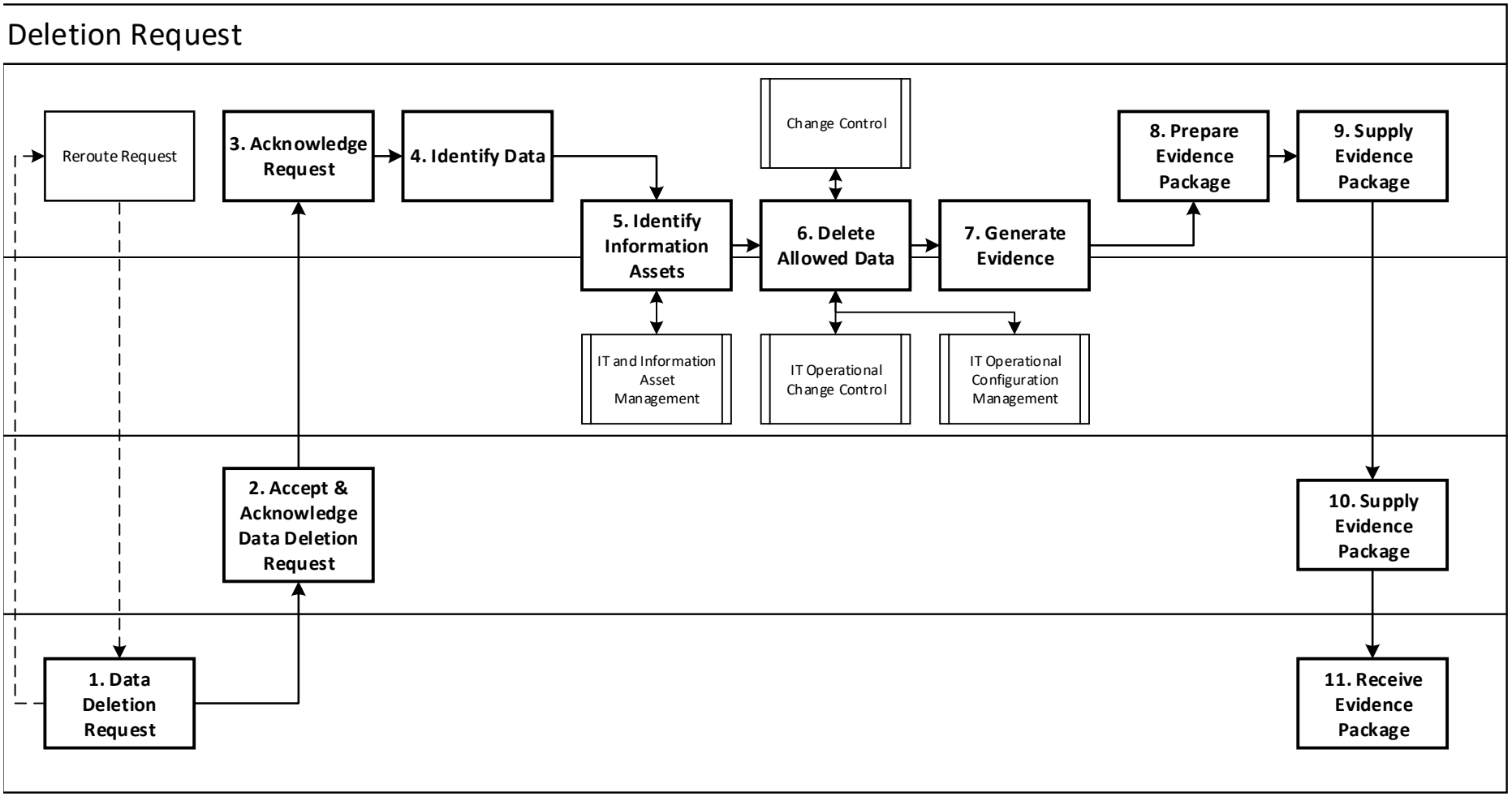
Note that because children may not have been able to fully appreciate the risks of providing consent while a minor, additional consideration should be given to requests to delete data when the data relates to a young person, regardless of their age at the time of the deletion request.

Cheshire Young Carers 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 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)
- Archiving purposes in the public interest, scientific research historical research or statistical purposes (e.g. data of historical significance)
- The exercise or defence of legal claims (e.g. complaints data, employment records, financial records etc)

Where such requests are refused, Cheshire Young Carers will 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

Step	Description
1. Data Deletion Request	The Data Subject makes a data subject deletion request. This should be directed to the office (any member of staff of any other volunteer, including the data owner (Responsible officer - Graham Phillips should direct the request to administration).
2. Accept and Acknowledge Data Deletion request	The office should immediately acknowledge receipt of the data subject deletion request. The office 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 office may, in consultation with the Nominated data controller (Martin Howlett) (Martin Howlett), refuse a data deletion request as outlined above. Where the scope of the request is not specific, the office should seek to clarify the scope of the request i.e. exactly what data should be deleted. The office should inform the Nominated data controller (Martin Howlett) that a data subject deletion request has been received and the Nominated data controller (Martin Howlett) should provide support and guidance as needed. The office should determine, with support from the Nominated data controller (Martin Howlett) whether the data subject deletion request is complex or simple. If the request is considered complex (see Annex 1), the office 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 office should inform the data subject that the data will be deleted within 1 month. The office should inform the data owner(s) (Responsible officer - Graham Phillips) of the data subject deletion request.
3. Acknowledge Request	The data owner(s) (Responsible officer - Graham Phillips) should acknowledge the data correction deletion to the office and prioritise their activities accordingly
4. Identify Data	Based upon the defined scope of the data subject deletion request, the data owner(s) (Responsible officer - Graham Phillips) 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 officer - Graham Phillips), the data owner(s) and 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 web part [list, folder, database]) • Other system or database (e.g. CRIS) Note that at this stage it may be discovered that data may have been shared with third parties. 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 officer -

Step	Description
	Graham Phillips) and 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. 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 officer - Graham Phillips) or data subject as appropriate.
7. Generate Evidence	The data owner(s), assisted by the 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 officer - Graham Phillips) 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 officer - Graham Phillips) should supply the evidence package 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 account and User ID).
10. Supply Evidence Package	The 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

Cheshire Young Carers 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 archive at the office
- Any request involving a combination of electronic and hard copy data
- Any request involving multiple data stores from within the Office 365 environment (e.g. email accounts, OneDrive folders, SharePoint sites [lists, folders, databases])
- Any request involving an Office 365 data store and any other system (e.g. CRIS)
- Any request involving data held by 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 Nominated data controller (Martin Howlett), balancing the rights of the data subject and the ability to correct the data, will provide a definitive determination of whether a data subject correction request is considered simple or complex.

Data Subject Correction Request Procedure

About this procedure

This procedure defines how Cheshire Young Carers will manage data subject requests to correct (rectify) erroneous or incomplete data in accordance with the Data Protection Act 2018. It should be read in conjunction with current information and guidance published by the UK Information Commissioner's Office (ICO – http://ico.org.uk/)

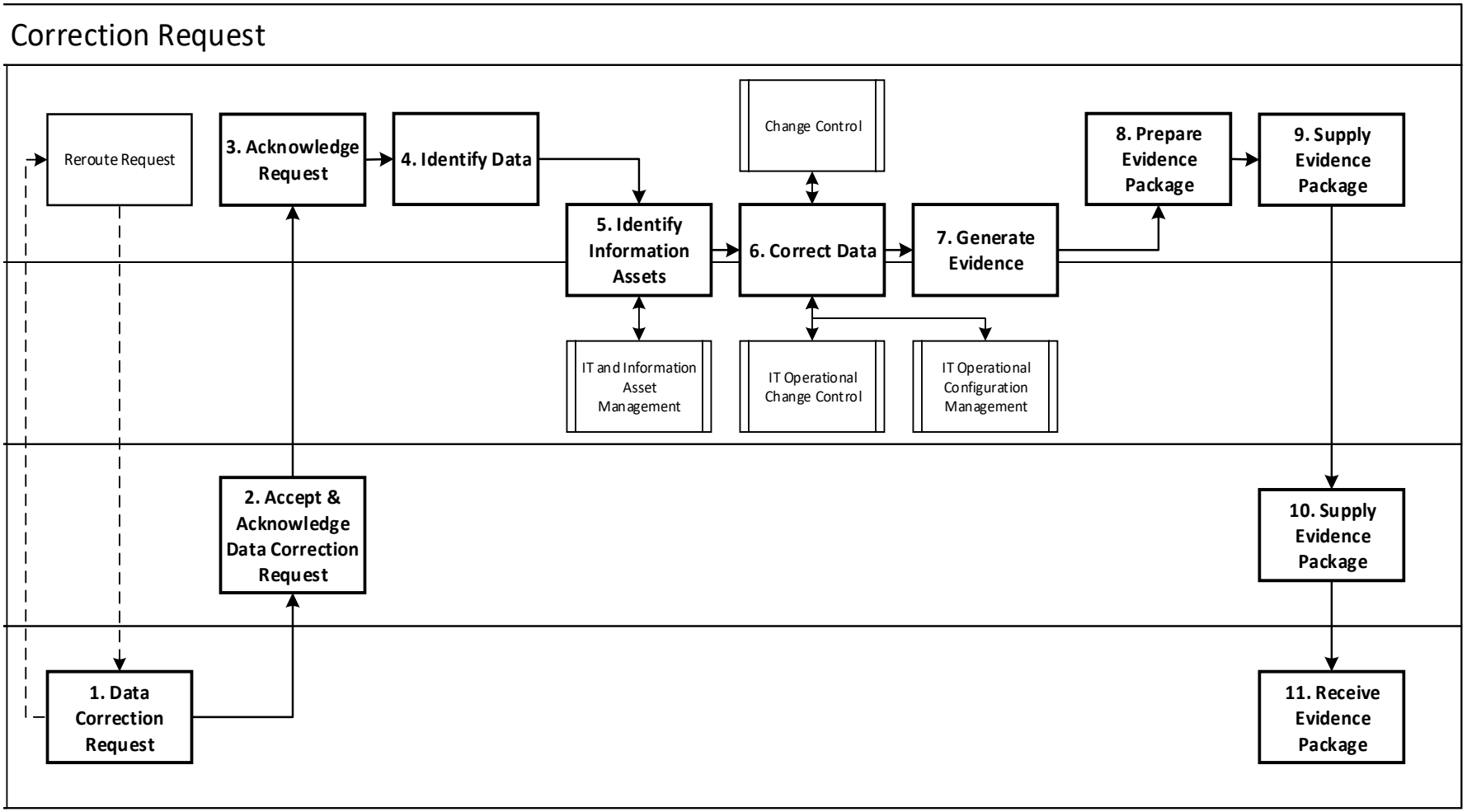
Note that now the UK has left the European Union, additional requirements of the European Union General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) may continue to apply with respect to data processed relating to EU citizens, which may include members, staff, suppliers, customers etc. As Cheshire Young Carers does not regularly process data relating to citizens of the EU as a matter of course, it is considered that the Data Protection Act 2018 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 GDPR Policy.

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

Cheshire Young Carers may choose not to correct subject data where it 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 office 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

Step	Description
12. Data Correction Request	The Data Subject makes a data subject correction request. This should be directed to the office (any member of staff of any other volunteer, including the data owner (Responsible officer - Graham Phillips) should direct the request to the office.
13. Accept and Acknowledge Data Correction request	The Office should immediately acknowledge receipt of the data subject correction request. The Office should maintain a log of all requests including: • Date request received • Data subject name and contact details • Scope of data subject correction request • Date of request acknowledgement • Date data correction confirmed The Office may, in consultation with the Nominated data controller (Martin Howlett), refuse a data correction request as outlined above. Where the scope of the request is not specific, the Office should seek to clarify the scope of the request i.e. exactly what data is incorrect and what the correct data should be. The Office should inform the Nominated data controller (Martin Howlett) that a data subject correction request has been received and the Nominated data controller (Martin Howlett) should provide support and guidance as needed. The Office should determine, with support from the Nominated data controller (Martin Howlett), whether the data subject correction request is complex or simple. If the request is considered complex (see Annex 1), the Office should inform the data subject that the request is complex and that the requested data will be corrected within 90 days. If the request is not considered complex (see Annex 1), the Office should inform the data subject that the data will be corrected within 1 month. The Office should inform the data owner(s) (Responsible officer - Graham Phillips) of the data subject access request.
14. Acknowledge Request	The data owner(s) (Responsible officer - Graham Phillips) should acknowledge the data correction request to the Office and prioritise their activities accordingly
15. Identify Data	Based upon the defined scope of the data subject correction request, the data owner(s) (Responsible officer - Graham Phillips) should identify the specific datasets that need to be corrected.
16. Identify Information Assets	Based upon the defined scope of the data subject correction request, and the datasets identified by the data owner(s) (Responsible officer - Graham Phillips), the data owner(s) and office 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 web part [list, folder, database]) • Other system or database (e.g. CRIS) 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.

17. 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 officer - Graham Phillips) and office 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 officer - Graham Phillips), Office or data subject as appropriate.
18. Generate Evidence	The data owner(s) (Responsible officer - Graham Phillips), assisted by the office 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.
19. Prepare Evidence Package	The data owner(s) (Responsible officer - Graham Phillips) 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.
20. Supply Evidence Package	The data owner(s) (Responsible officer - Graham Phillips) should supply the evidence package to the Office 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. using a temporary, read only account and User ID).
21. Supply Evidence Package	The Office 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.
22. 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

Cheshire Young Carers 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 a combination of electronic and hard copy data
- Any request involving multiple data stores from within the Office 365 environment (e.g. email accounts, OneDrive folders, SharePoint sites [lists, folders, databases])
- Any request involving Office 365 data store and any other system (CRIS)
- Any request involving data held by 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 Nominated data controller (Martin Howlett), balancing the rights of the data subject and the ability to correct the data, will provide a definitive determination of whether a data subject correction request is considered simple or complex.

Data Subject Access Request Procedure

About this procedure

This procedure defines how Cheshire Young Carers will manage data subject access requests in accordance with the Data Protection Act 2018. 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 now the UK has left 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 Cheshire Young Carers does not regularly process data relating to citizens of the EU as a matter of course, it is considered that the Data Protection Act 20918 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 GDPR Policy.

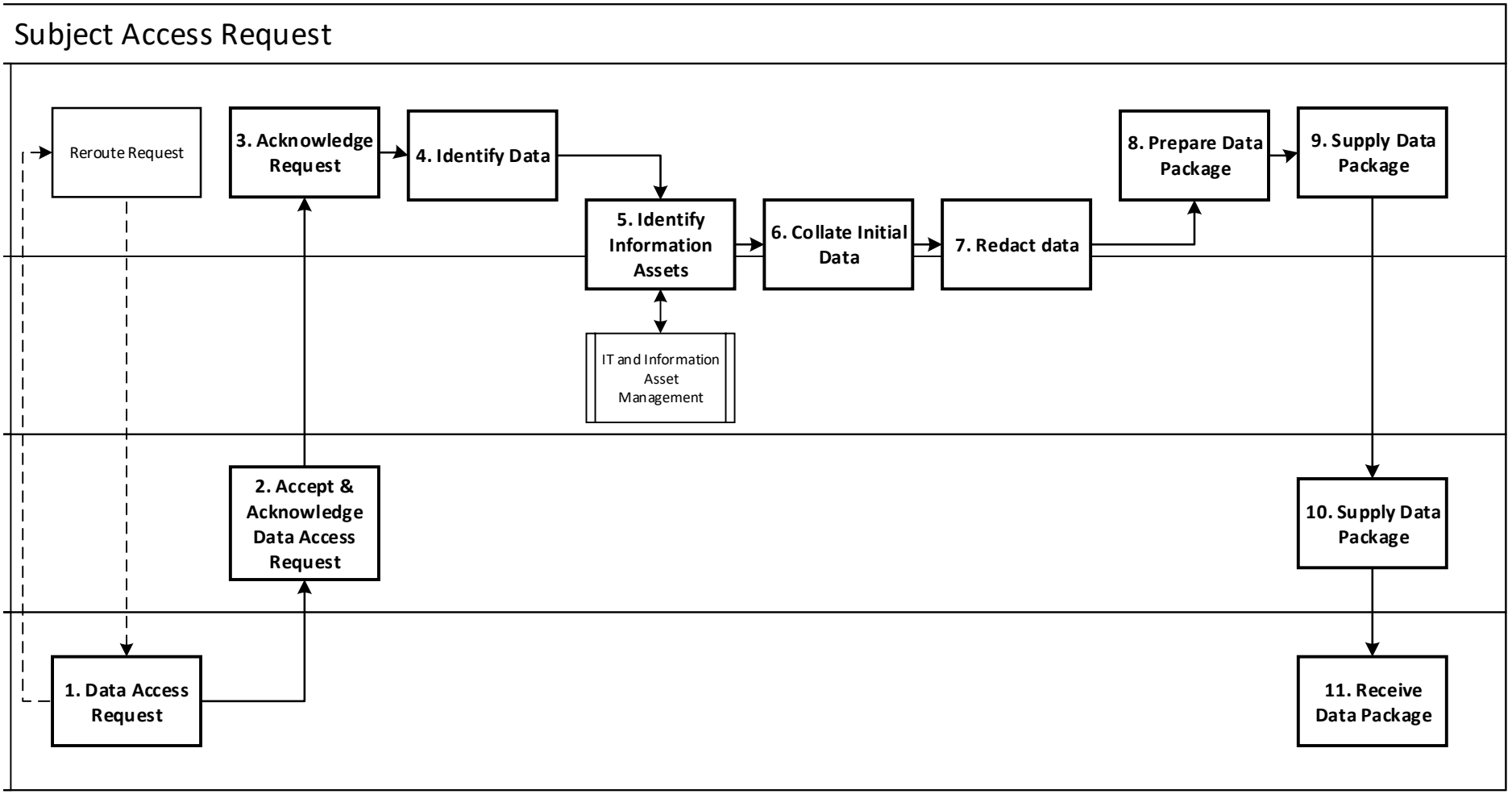
Where the office is known to hold no data about a data subject, this should clearly be communicated upon request.

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.

Cheshire Young Carers 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, it 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 Cheshire Young Carers is a not for profit charity, Cheshire Young Carers reserves the right to charge a reasonable fee (based upon a volunteer rate of £20.00/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

Step	Description
23. Data Access Request	The Data Subject makes a data subject access request. This should be directed to the Office (any member of staff of any other volunteer, including the data owner (Responsible officer - Graham Phillips) should direct the request to the Office.
24. Accept and Acknowledge Data Access request	The Office should immediately acknowledge receipt of the data subject access request. The Office 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 Office may, in consultation with the Nominated data controller (Martin Howlett), refuse or charge for a request as outlined above. Where the scope of the request is not specific, the Office should seek to clarify the scope of the request i.e. whether it relates to all data held by Cheshire Young Carers, or to a specific subset of data (specific datasets, timescales, relating to specific events etc) The Office should inform the Nominated data controller (Martin Howlett) that a subject access request has been received and the Nominated data controller (Martin Howlett) should provide support and guidance as needed. The Office should determine, with support from the Nominated data controller (Martin Howlett), whether the data subject access request is complex or simple. If the request is considered complex (see Annex 1), the Office 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 Office should inform the data subject that the requested data will be provided within 1 month. The Office should inform the data owner(s) (Responsible officer - Graham Phillips) of the data subject access request.
25. Acknowledge Request	The data owner(s) (Responsible officer - Graham Phillips) should acknowledge the request to the Office and prioritise their activities accordioning
26. Identify Data	Based upon the defined scope of the data subject access request, the data owner(s) (Responsible officer - Graham Phillips) should identify the specific datasets that need to be accessed
27. Identify Information Assets	Based upon the defined scope of the data subject access request, and the datasets identified by the data owner(s) (Responsible officer - Graham Phillips), the data owner(s) and office 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 web part [list, folder, database]) • Other system or database (e.g. CRIS)
28. 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 officer - Graham Phillips) and office Administrator will collate data and records within the scope of the request (as hard copies and/or a separate electronic copy)

Step	Description
29. Redact Data	The data owner(s) (Responsible officer - Graham Phillips), assisted by the office 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 personal details) • 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.
30. Prepare Data Package	The data owner(s) (Responsible officer - Graham Phillips) 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.
31. Supply Data Package	The data owner(s) (Responsible officer - Graham Phillips) should supply the data package to the Office 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 charity account and User ID).
32. Supply Data Package	The Office 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.
33. 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

Cheshire Young Carers 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 charity Office 365 environment (e.g. email accounts, OneDrive folders, SharePoint sites [lists, folders, databases])
- Any request involving Office 365 data store and any other system (e.g. CRIS)
- Any request involving data held by charity 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 Nominated data controller (Martin Howlett), balancing the rights of the data subject and the ability of the charity to access, redact and provide data, will provide a definitive determination of whether a data subject access request is considered simple or complex.

Data Privacy Management Procedure

About this procedure

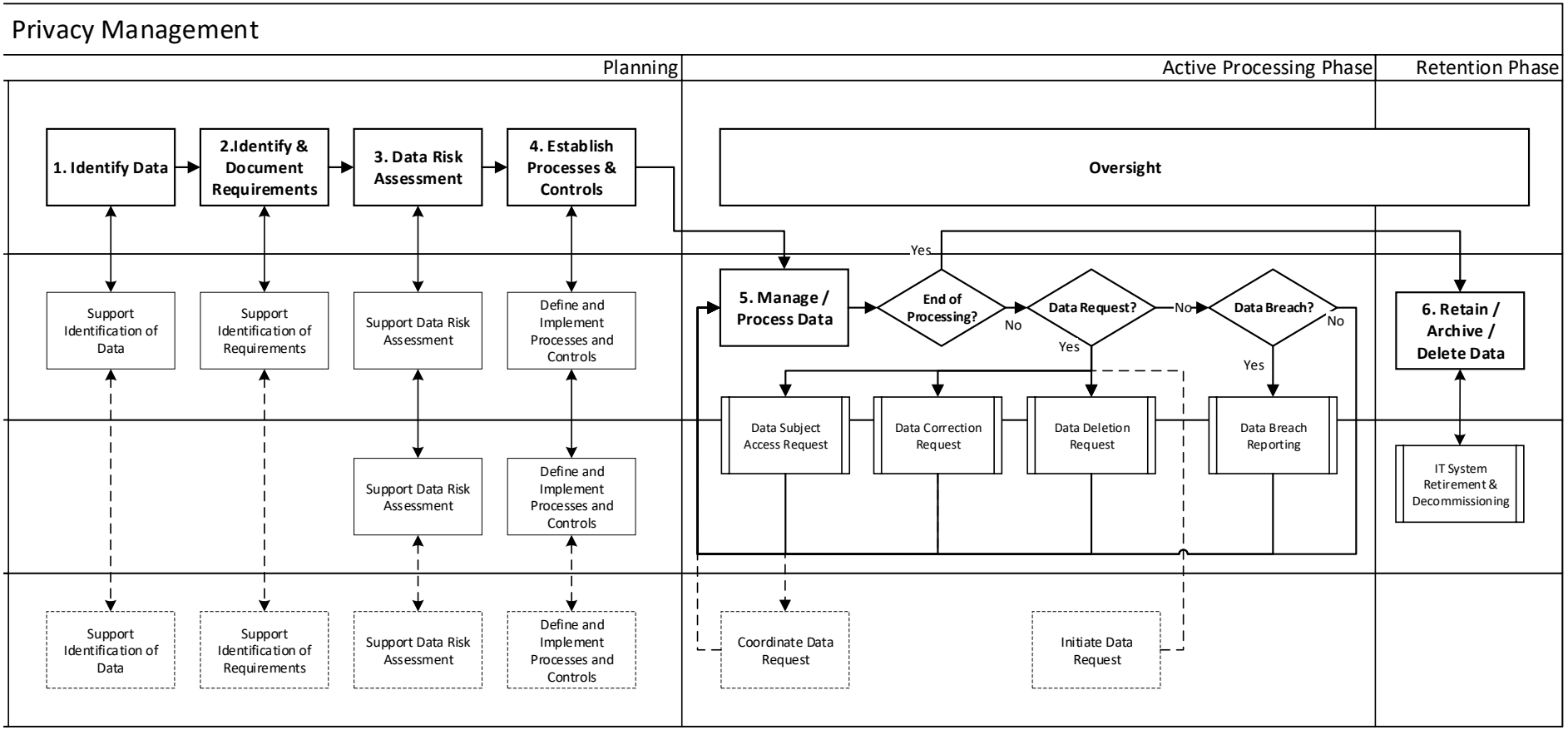
This procedure defines how Cheshire Young Carers will manage personal data to assure appropriate data privacy in accordance with the Data Protection 2018. It should be read in conjunction with current information and guidance published by the UK Information Commissioner's Office (ICO – http://ico.org.uk/)

Note that now the UK has leftthe 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 Cheshire Young Carers does not regularly process data relating to citizens of the EU as a matter of course, it is considered that the Data Protection Act 2018 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 charity GDPR 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
34. Identify Data	The Nominated data controller (Martin Howlett) is responsible for identifying all personal data, supported by the appropriate Responsible officer - Graham Phillips (data owner) and other appropriate volunteers or members of staff. For each set of personal data processed, the charity GDPR policy defines: • The data description • The personal data included • How and where data is stored • The data retention policy • The Responsible officer - Graham Phillips (data owner) Where new data sets or changes to datasets (including data no longer held) are identified, the GDPR policy should be updated to reflect the changes and steps 2 – 4 (and possibly step 6) repeated for the dataset
35. Identify and Document Requirements	For all personal data, the Nominated data controller (Martin Howlett) is responsible for identifying data protection and data privacy requirements, supported by the appropriate Responsible officer - Graham Phillips (data owner) and other appropriate volunteers or members of staff. These are generally based on the requirements derived from the UK Data Protection Act 2018. 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.
36. Data Risk Assessment	The Nominated data controller (Martin Howlett) is responsible for ensuring that data privacy risks are identified, supported by the appropriate Responsible officer - Graham Phillips (data owner), other appropriate volunteers or members of staff including the office 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. Cheshire Young Carers 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.
37. Establish Process and Controls	General data protection principles and controls are defined in the charity GDPR 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

Step	Description
	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
38. 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 charity GDPR policy. Any specific data privacy management actions will be conducted in accordance with the following procedures: • Subject Data Access Request Procedure • Subject Data Correction Request Procedure • Subject Data Deletion Request Procedure • Subject Data Breach Reporting Procedure In addition, the following rights must be respected: **Right to Object** Individuals should be informed of their right to object to data processing at the first point of communication i.e. the first email they receive, available on their first visit to a website etc. Individuals may object to: • Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); • Direct marketing (including profiling) e.g. Moor House Adventure Centre mailings • Processing for purposes of scientific/historical research and statistics. In these cases, processing must cease unless Cheshire Young Carers 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:

Step	Description
	• 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 Charity's legitimate grounds override those of the individual. • When processing is unlawful and the individual opposes erasure and requests restriction instead. • If the charity 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 Cheshire Young Carers; • 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 (Martin Howlett)) 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)
39. Retain / Archive / Delete Data	Following the ending of active processing a decision will be made to either retain, archive or delete data as follows: • Retain data: For cases where data is no longer being actively updated, changed or added to, but which still needs to be referred to on a regular basis. Where this is the case, access controls and permissions should be updated to make data 'read only' where possible • Archive data: For cases where data is no longer being actively updated, changed or added to, and which does not need to be referred to on a regular basis (i.e. may be retained for statutory purposes, risk mitigation purposes etc). Where this is the case, access controls and permissions should be updated to make data 'read only' where possible and the data should be moved to a suitable secure hard copy of electronic archive • Delete data: For cases where data no longer needs to be retained When considering the above it should be recognised that data may progress through a natural life cycle (active processing ➔ retained ➔ archived ➔ deleted), possibly bypassing these steps. Data should not be retained beyond the retention period defined in the charity data retention policy

Annex 1 – General Data Privacy Impact Assessment

Cheshire Young Carers has determined the need for a Data Privacy Impact Assessment (PIA). This is because Cheshire Young Carers:

- 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) 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

Cheshire Young Carers 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 2018 (and EU GDPR) Inability to comply with Policy, Organisation and Rules of the Charity	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 charity GDPR policy.

Annex 2 – Complex Data Portability Requests

Cheshire Young Carers 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 charity Office 365 environment (e.g. email accounts, OneDrive folders, SharePoint sites [lists, folders, databases])
- Any request involving a charity Office 365 data store and any other system (e.g. CRIS)
- Any request involving data held by charity 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 Nominated data controller (Martin Howlett), balancing the rights of the data subject and the ability of the charity to transfer the data, will provide a definitive determination of whether a data transfer request is considered simple or complex.

Data Breach Reporting Procedure

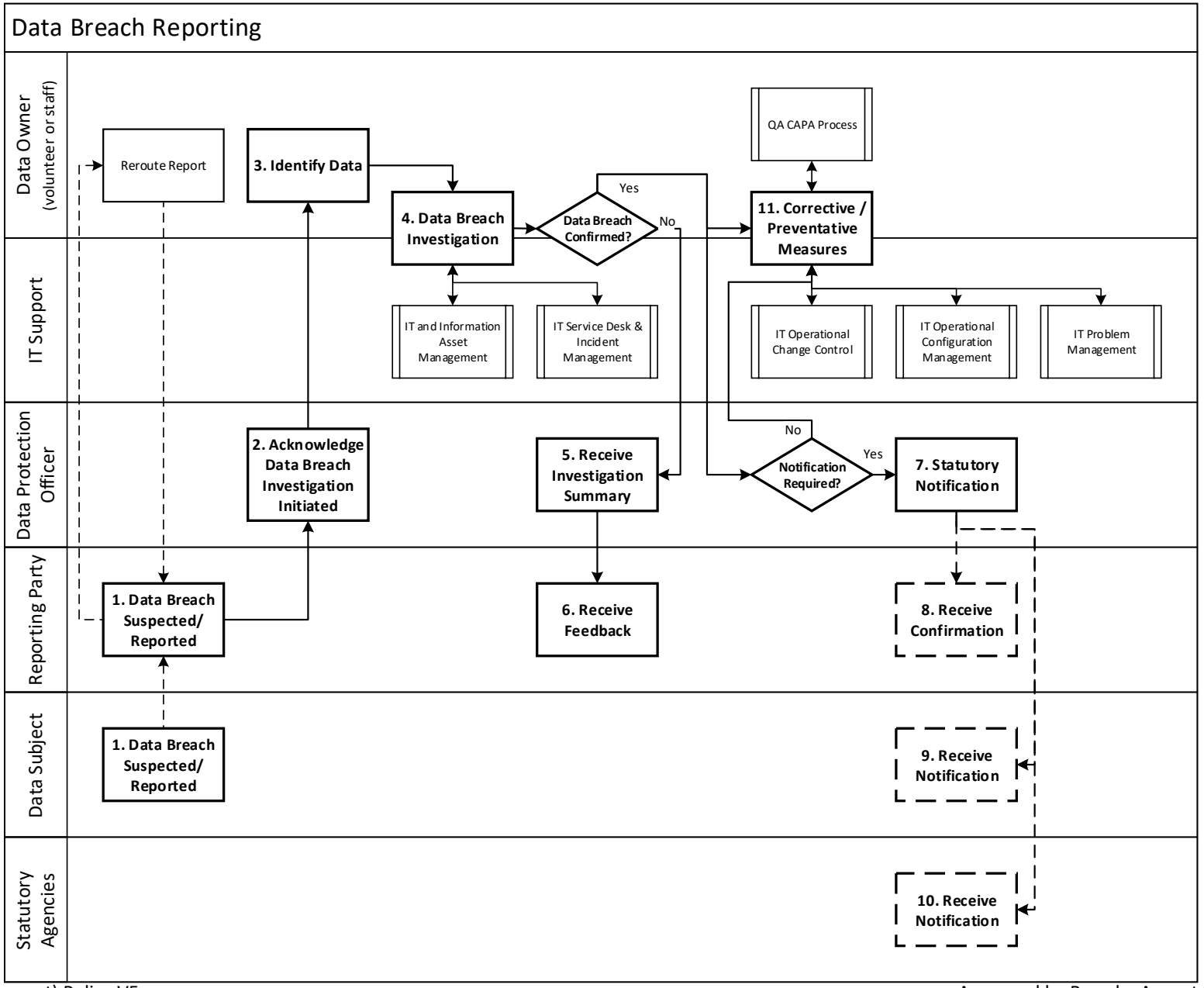
About this procedure

This procedure defines how Cheshire Young Carers 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 now the UK has left 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 Cheshire Young Carers does not regularly process data relating to citizens of the EU as a matter of course, it is considered that the Data Protection Act 2018 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 charity GDPR Policy.

Note that any sub processors engaged on behalf of Cheshire Young Carers (e.g. facilitators, professional partners 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
40. Data Breach Suspected / Reported	The data subject, or any other party reports a suspected or actual personal data breach. All staff and volunteers of Cheshire Young Carers 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 Nominated data controller (Martin Howlett). Any other member of staff or any other volunteer receiving such a report should request the reporting party to report the matter to the Nominated data controller (Martin Howlett) and copy the Nominated data controller (Martin Howlett) will all correspondence.
41. Acknowledge Data Breach Investigation Initiated	Upon receiving any report of an actual or suspected data breach, the Nominated data controller (Martin Howlett) 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 - Graham Phillips) should be informed of the actual or suspected breach. The Board and CEO should also be informed.
42. Identify Data	The Data Owner(s) (Responsible officer - Graham Phillips) will identify the scope of the actual or suspected data breach. The office Administrator will provide support to identify the IT and information assets potentially involved.
43. Data Breach Investigation	The office Administrator will provide support to identify the IT and information assets potentially involved. The Data Owner(s) (Responsible officer - Graham Phillips) 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 pseudonymising, damage to reputation, loss of confidentiality of*

Step	Description
	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. This may leverage any IT incident management procedures.
44. Receive Investigation Summary	If personal data privacy was NOT breached, the Data Owner(s) (Responsible officer - Graham Phillips) should send a brief summary of the investigation to the Nominated data controller (Martin Howlett), including the reasons for concluding that personal data privacy was not breached
45. Receive Feedback	If personal data privacy was NOT breached, the Nominated data controller (Martin Howlett) should send a summary of the investigation to the reporting party, including the reasons for concluding that personal data privacy was not breached. The Board and CEO should also be informed.

46. Statutory Notification	If personal data privacy WAS breached, the impact of the breach should be determined by the Nominated data controller (Martin Howlett). If the Nominated data controller (Martin Howlett) 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 Nominated data controller (Martin Howlett) 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, 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.
47. Receive Confirmation	If personal data privacy WAS breached, the Nominated data controller (Martin Howlett) should send a summary to the reporting party, confirming that the matter is being treated as a data privacy breach. The Board and CEO should also be informed.
48. 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 Nominated data controller (Martin Howlett) 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 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
49. 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.
50. 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 involve IT change management or configuration management processes