The Grenfell Club
inspiring lives

GDPR

DATA PROTECTION POLICIES AND PROCEDURES

MAY 2018

The Grenfell Club
inspiring lives

Contents

DATA ACCEPTABLE USE POLICY 3

1. SCOPE 3

2. POLICY 3

DATA RETENTION POLICY 4

1. Scope 4

2. Responsibilities 4

3. Policy 4

4. Review 5

DATA PORTABIITY, RECTIFICATION & ERASURE POLICIES 6

5. SCOPE 6

6. DATA PORTABILITY 6

7. DATA RECTIFICATION 6

8. DATA ERASURE 7

8.7. **Out of scope** 8

8.8. **Timeframes** 8

8.9. **Fees** 8

9. THE RIGHT TO OBJECT 9

9.1. **SCOPE** 9

9.2. **PROCEDURE** 9

9.6. **Direct Marketing** 9

9.7. **Research** 9

9.8. **Online** 9

THE RIGHT TO RESTRICT PROCESSING 10

10. SCOPE 10

10.9. **Other Parties** 10

DATA SUBJECT ACCESS REQUEST POLICY 11

11. SCOPE 11

12. RECEIVING A SUBJECT ACCESS REQUEST (SAR) 11

13. PROCESSING SAR's 11

14. FEES 12

15. EXCESSIVE REQUESTS 12

DEALING WITH & REPORTING BREACHES 13

16. SCOPE 13

16.5. **Personal Data Breaches** 13

17. Reporting a Breach - Procedures 14
Preparing for a personal data breach 15
Responding to a personal data breach 16
19. Reporting a breach to Individuals 16
20. CLEAR DESK & SCREEN 17
20.1.8. Reduction in the use of paper: 19
20.1.9. Tips for having a clear desk 19
APPENDIX 1. 20
PERSONAL DATA CONSENT FORM 20
APPENDIX 2. 21
DATA SUBJECT ACCESS REQUEST FORM 21

DATA ACCEPTABLE USE POLICY

1. SCOPE

1.1. Under the GDPR, data subjects have a right to know who has access to their personal data, where that data is stored and precisely what that data will be used for.

1.2. The Grenfell Club will always ensure that its' employees, volunteers and trustees and any third-party organisations are aware of limitations on the storage and use of personal data.

2. POLICY

2.1. Following an objection being raised you must stop processing personal data.

2.1.1. Employees, volunteers and trustees may routinely, during the course of their work, store such personal data as:

- Name
- Address
- Telephone Number
- Email Addresses
- Mobile Numbers
- Emergency contact details
- Referral Forms (containing personal details)
- GP information
- Disability and medication
- Bank details (employees)

2.1.2. Data is stored in paper form and electronically on computers.

2.1.3. Particularly owing to the 'Special Category' nature of some of the data stored, employees, volunteers and trustees must not store any personal data on private data sticks.

2.1.4. Where employees, volunteers and trustees, have good cause to store some personal data on a personal mobile phone, the device must be encrypted and protected by passcode, pin and/or biometrically and it must be deleted in line with the charity's data erasure policy, as soon as it is required.

2.1.5. Employees, volunteers and trustees, volunteers and trustees may not store personal data of individuals on their own personal devices such as, laptops, desktops, tablets etc.

2.1.6. Paper documentation containing personal data should never be removed from the charity's office without prior authorisation, nor should it be copied without the same.

2.1.7. Authorisation must first be obtained from the data controller and only for the intended business use.

2.1.8. All steps should be taken by employees, volunteers and trustees to protect personal data in their possession through deploying adequate security measures, by using encryption, password protection and restricting access and securing documents in their possession.

DATA RETENTION POLICY

Under the terms of the General Data Protection Regulation, it is incumbent on companies and organisations to ensure that personal data is only stored for as long as is absolutely necessary.

The Grenfell Club ("the charity"), will ensure that all employees, volunteers and trustees will be made aware of and will receive training in the charity policy with regard to retention of data and that this policy will remain GDPR compliant.

1. Scope

1.1. All of The Grenfell Club's personal data records, whether digitised or in paper form will remain subject to this policy.

2. Responsibilities

2.1. The following shall bear overall and joint responsibility for the retention and decisions around retention of personal data within the charity:

2.1.1. The Data Controller

2.1.2. The Charity Directors

2.1.3. The Data Protection Officer

2.2. Additionally, employees, volunteers and trustees of the charity will bear responsibility for all personal data processed respectively and will adhere to this policy accordingly.

3. Policy

3.1. All personal data processed and stored by The Grenfell Club, shall be held securely with access restricted to essential personnel and according to the charity's terms and conditions, which are and shall remain GDPR compliant.

3.2. Such data held by the charity shall, where there exist statutory obligations, be held for as long as legally required and shall adhere with and held for the purposes of:

3.2.1. Charitable Trust Regulations

3.2.2. HMRC requirements

3.2.3. Employment legislation

3.2.4. Duty of care obligations

3.2.5. Any and all other statutory or legal requirements

3.3. All other personal data, in the absence of any legal requirements, shall only be retained for as long as is necessary to complete the purpose for which it has been stored, after which it must be deleted within one month from when:

3.3.1. A request from the data subject to erase their personal data has been received.

3.3.2. The data subject has withdrawn their consent for the data to be processed or stored

3.3.3. The contract or transaction has been completed and can no longer be performed

3.3.4. The information contained within is no longer relevant or is out of date

3.4. Exceptions may apply to the processing for historical, statistical or scientific purposes, under which circumstances the data must be anonymised by an acceptable form of redaction.

3.5. During the period of retention personal data must be reviewed every 6 months in line with the following:

3.5.1. Genuine business requirements or professional standards

3.5.2. Ongoing processing purposes

3.5.3. Legal requirements

3.6. Should none of the above reasons be valid at the time of review, the data should be destroyed.

3.7. Should the data review period expire, it may also be acceptable to:

3.7.1. erase the unique identifiers that allow the allocation of the data set to a unique person;

3.7.2. erase single pieces of information that identify the data subject (whether alone or in combination with other pieces of information);

3.7.3. separate personal data from non-identifying information (e.g. an order/ID number from the customer's name and address); or

3.7.4. aggregate personal data in a way that no allocation to any individual is possible.

3.8. All actions pursuant to clauses 3.6 and 3.7 must have prior Director authorisation and must be accomplished as per specific instructions from the Data Controller.

3.9. Erasure and destruction of personal data, once authorised, must be accomplished in the following manner:

3.9.1. Paper will be shredded using a cross-cut shredder or, collected by the charity's appointed data elimination body, which must be GDPR compliant.

3.9.2. Electronically stored data on laptops or desktops will be destroyed by the charity's I.T. provider upon instruction by the Data Controller.

3.9.3. Any information stored by any other electronic means, e.g. smart phones, data sticks, external hard drives, tablets etc., must be submitted to the charity and will be erased permanently by the charity's I.T. provider upon instruction from the Data Controller.

3.9.4. Any data held on the above devices in clause 3.9.3, must have been stored following authorisation from the Data Controller. Without such authorisation you may not store personal data on any of those devices and a failure to adhere to this policy will lead to a charge of gross misconduct and disciplinary action will be taken.

3.10. At the time of submitting their personal data, all data subjects should be informed of:

3.10.1. The period that their data will be retained for.

3.10.2. The purpose of retention of their personal data for that period.

3.10.3. The new retention period if the purpose of processing has changed after personal data has been obtained.

4. Review

4.1. This policy will be reviewed for effectiveness on an annual basis and may be updated or revised as required.

5. SCOPE

5.1. Under the GDPR, data subjects have the right to obtain and reuse their personal data for their own purposes across different services.

5.2. Furthermore, upon accessing their personal data, data subjects have the right to have their data rectified if it is inaccurate or incomplete. They may also have the right to request the deletion or removal of personal data where there is no compelling reason for its' continued processing.

5.3. This policy will be completely adhered to by The Grenfell Club and all its' employees, volunteers, trustees and representatives.

5.4. The Grenfell Club shall have procedures in place to ensure that individuals' rights of portability, rectification and erasure are met within a timely and appropriate manner.

6. DATA PORTABILITY

6.1. When a request for data to be accessed to be reused for other purposes by the individual, the request must be dealt with promptly, within 30 days.

6.2. To enable other organisations to be able to use that data, it must be in a suitable machine-readable format, such as CSV, Excel etc.

6.3. If you are requested to transfer the data directly to another organisation by the data subject and it is technically possible and feasible to do so, this would be acceptable, but take steps to ensure that the data is transmitted in an encrypted format.

6.4. If the data concerns more than one individual and you consider the rights of the other individual(s) may be at risk, you should either refuse to send the data or, whenever possible, redact the data to protect the rights of the other person(s).

6.5. Although a response must be given without undue delay and within one month, this can be extended by two months where the request is of a complex nature or you receive a number of requests. However, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

6.6. Where you will not be taking action in response to a request, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

7. DATA RECTIFICATION

7.1. Under the GDPR Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

7.2. If personal data has been disclosed in question to other parties, you must contact each recipient and inform them of the rectification, unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the data subject about these recipients.

7.3. You must respond within one month to any such requests but may extend this time by a further two months where the request for rectification is complex.

7.4. Where you will not be taking action in response to a request, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.

8. DATA ERASURE

8.1. Under the GDPR, individuals have the right to have their personal data permanently erased, also referred to as "the right to be forgotten". Organisations must comply with these requests when there is no compelling reason for continuing to process personal data.

8.2. For The Grenfell Club, there are specific circumstances where the right to have personal data erased and to prevent processing applies, namely:

8.2.1. Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.

8.2.2. When the individual withdraws their consent with valid reason.

8.2.3. When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.

8.2.4. The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).

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

8.3. **When it is right to refuse a request for erasure**

8.3.1. A request for erasure can be refused where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information.;
- to comply with a legal or statutory obligation, for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

8.4. Any refusal to comply with a request for data to be erased must have prior approval from the Charity Manager or a charity trustee.

8.5. Similarly, all data erasure requests that are complied with must also seek director approval but within given timescales.

8.6. **Erasing data**

8.6.1. Once it has been determined that there are no known reasons that the request for erasure cannot be complied with, data processors, after authorisation from the data controller will locate all storage locations of the personal data, which may include electronically stored data on laptops, desk tops, tablets, smart phones, data sticks etc., or within paper files.

8.6.2. Electronically stored data:

8.6.2.1. For all such data a request should be made to the charity's I.T. provider to permanently delete any data after taking steps to erase the data locally.

8.6.3. Paper data:

8.6.3.1. For all such data a request should be made to remove the paper files and permanently delete any data by use of a cross-cut shredder.

8.6.4. Verification that all data has been deleted as requested by the data subject, should be obtained from all parties carrying out the deletions.

8.7. **Out of scope**

8.7.1. Non-electronic documents which are not (or not to be) filed, (e.g. it is data that is not searchable), e.g. a random piece of microfiche, or a paper notepad, are not classed as personal data under the GDPR and are therefore not subject to the right to erasure.

8.8. **Timeframes**

8.8.1. All data erasure requests must receive a response without "undue" delay and, "at the latest within one month".

8.8.2. If the controller decides not to comply with the request because there is a legitimate right to refuse, then the data subject must be advised of this within the same timeframe, be given the reasons for this.

8.9. **Fees**

8.9.1. With very limited exceptions (such as SAR requests which are "manifestly unfounded") all data erasure requests must be dealt with without any charge to data subjects.

9. THE RIGHT TO OBJECT

9.1. SCOPE

9.1.1. Under the GDPR, data subjects have a right to object to the following:

- processing that is based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for the purposes of scientific/historical research and statistics.

9.1.2. When data processing is objected to, it is important that data subjects must have an objection based on "grounds relating to his or her particular and specific situation". This is especially so where you process personal data for the performance of a legal task or for the charity's legitimate interests.

9.2. PROCEDURE

9.2.1. Following an objection being raised you must stop processing personal data unless:

- you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.
- You must explicitly inform individuals of their right to object at the point of first at which they communicate with the charity and in it must also feature clearly and separately from any other information in the charity's privacy notice.

9.6. Direct Marketing

9.6.1. No employee, volunteer or trustee of The Grenfell Club may continue processing personal data for direct marketing purposes after having received an objection.

9.6.2. There are no exemptions or grounds to refuse.

9.6.3. Employees, volunteers and trustees must deal with an objection to processing for direct marketing at any time and free of any charge.

9.7. Research

9.7.1. Data subjects must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes.

9.7.2. If the charity is conducting research where the processing of personal data is necessary for the performance of a public interest task, there is no requirement to comply with an objection to the processing.

9.8. Online

9.8.1. Should processing activities fall into any of the above categories and are carried out online, there must be a way for data subjects to object online.

9.8.2. The charity will work with third party organisations and its I.T. provider to ensure this method of objection exists.

9.8.3. All Grenfell Club employees, volunteers and trustees will inform data subjects of the ability to object online to direct marketing and/or research that is online-based.

THE RIGHT TO RESTRICT PROCESSING

10. SCOPE

10.1. Under the GDPR, data subjects have a right to 'block' or suppress the processing of their personal data.

10.2. When data processing is restricted, you are permitted to store the personal data, but not to further process it.

10.3. Organisations may retain just sufficient information about the individual to ensure that the restriction is respected in future.

10.4. The Grenfell Club must have procedures in place to ensure that individuals' rights of restriction of processing are met in an appropriate manner.

Restriction of personal data is required by The Grenfell Club under the following circumstances:

10.5. Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.

10.6. Where 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 you are considering whether your organisation's legitimate grounds override those of the individual.

10.7. When processing is unlawful and the individual opposes erasure but requests restriction instead.

10.8. If the charity no longer requires the personal data but the individual requires the data to establish, exercise or defend a legal claim.

10.9. **Other Parties**

10.9.1. If disclosure of the personal data in question has been made to other parties, each recipient must be contacted and informed of the restriction on the processing of the personal data, unless this proves impossible or involves unreasonably disproportionate effort.

10.9.2. If requested to, you must also inform the data subject about these recipients of their data.

10.9.3. You must inform data subjects without undue delay when it has been decided to lift a restriction on processing.

DATA SUBJECT ACCESS REQUEST POLICY

11. SCOPE

11.1. Under the GDPR, all living individuals have the right to access their personal data and all supplementary information.

11.2. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

11.3. This policy will be completely adhered to by The Grenfell Club and all its' employees, volunteers and trustees and representatives.

11.4. The Grenfell Club is required to have procedures in place to ensure that individuals' rights of access are met within a timely and appropriate manner and seek to enable all who wish to do so to have access to the records that are held about them.

12. RECEIVING A SUBJECT ACCESS REQUEST (SAR)

12.1. When an SAR is received via telephone or email, a form should be sent to the person requesting access for completion and return.

12.2. Data subjects have the right to make their requests in other formats and may elect not to, or may not be physically able use the form. Should this situation arise, you should follow the procedures outlined in clause 13.3 to 13.5 below.

13. PROCESSING SAR's

13.1. The GDPR is very explicit about the time-period permitted for dealing with SAR's, therefore when an SAR has been received, it is imperative to inform the Data Subject that their request will be dealt with within 30 days and then to ensure that this happens.

13.2. If the data subject has completed a form and returned it, the total time from the original request must be included as part of the 30-day response period.

13.3. Owing to the reduced response time of 30 days, you should endeavour to contact the data subject within 3 to 4 days after sending the form, to confirm receipt and thereafter within a further 3 to 4 days if the form has not been returned, to request that it be returned.

13.4. Should the data subject elect not to use the form, or the form is not received within the office they should be contacted and asked the relevant questions from the form, which will then be completed by the person processing the request.

13.5. All forms and SAR's in other formats received at The Grenfell Club will be treated as personal data and appropriate storage and other security measures taken to protect the data.

13.6. All requested data must be tracked down from its' various storage locations and the following steps are to be considered prior to sending the data onwards:

13.6.1. Redact information relating to other individuals unless you have their consent, or it is reasonable in all the circumstances to provide that information.

13.6.2. Consider whether an exemption applies where the data would be exempt from disclosure.

13.6.3. Respond to the request within the timeframe, provide copies of the relevant data and explain if and why you are relying on any of the exemptions.

13.7. Once compiled, the data must be dispatched so that it arrives within 30 days of the original request via trackable means and using a method that requires a signature upon receipt of the package.

14. FEES

14.1. No organisation may now charge for complying with a request unless the request is considered to be 'manifestly unfounded or excessive'. However, a reasonable administrative-cost fee may be levied if further copies are requested.

15. EXCESSIVE REQUESTS

15.1. Should a request be deemed 'manifestly unfounded or excessive', the charity may charge a fee or refuse to respond but will need to be able to provide evidence of how the conclusion that the request is manifestly unfounded or excessive was reached.

15.2. Only the Data Controller (the charity directors), may make the decision as to whether or not a fee may be chargeable.

DEALING WITH & REPORTING BREACHES

16. SCOPE

16.1. Under the GDPR, there is a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. This needs to be done within 72 hours of becoming aware of the breach, where feasible.

16.2. Where the breach is likely to result in a high risk of adversely affecting the data subject's rights and freedoms, you must also inform those individuals without undue delay.

16.3. The Grenfell Club will put robust breach detection, investigation and internal reporting procedures in place, in order to decide whether or not it needs to notify the relevant supervisory authority and the affected individuals.

16.4. The Grenfell Club will also keep a record of any personal data breaches, regardless of whether it is required to notify.

16.5. **Personal Data Breaches**

16.5.1. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. Examples will include, but are not limited to:

- 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; and
- loss of availability of personal data.

16.5.2. There will always be a personal data breach whenever:

- any personal data is lost, destroyed, corrupted or disclosed;
- if someone accesses the data or passes it on without proper authorisation or;
- if the data is made unavailable and this unavailability has a significant negative effect on individuals.

16.5.3. Under Recital 87 of the GDPR, when a security incident takes place, the data controller must quickly establish whether a personal data breach has occurred and if so, promptly take steps to address it, including informing the Information Commissioners Office (ICO), if required.

16.5.4. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors. Potential consequences to data subjects may include:

- loss of control over their personal data or limitation of their rights,

- discrimination,
- identity theft or fraud,
- financial loss,
- unauthorised reversal of previously anonymised data (pseudonymisation),
- damage to reputation,
- loss of confidentiality of personal data protected by professional secrecy or;
- any other significant economic or social disadvantage to the person concerned.

16.6. Organisations must report a notifiable breach to the ICO without undue delay, but not later than **72 hours** after becoming aware of it. If you take longer than this, you must give good reasons for the delay. Section II of the Article 29 Working Party Guidelines on personal data breach notification provides more details of when a data controller can be considered to have "become aware" of a breach.

17. Reporting a Breach - Procedures

17.1. As soon as you become aware that a personal data breach has occurred, whether internally to the charity, or externally, you must inform the Charity Manager or a trustee should the manager be unavailable, immediately and without delay. Please refer to clauses 16.5.1 and 16.5.2 to see examples of the types of breaches that may occur.

17.2. Upon notification that a breach may have occurred, the data controller (director) must immediately commence an investigation, taking into consideration the following:

i. Date of the breach
ii. Nature of the breach
iii. Detailed description of the breach
iv. Number of people affected
v. How The Grenfell Club became aware of the breach
vi. Description of the data loss/theft etc.
vii. Potential consequences of the breach, particularly if special category data has been accessed.
viii. Whether all employees, volunteers and trustees and affected persons have or should be informed
ix. the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained.
x. Any remedial steps/actions taken or to be taken
xi. Has the ICO been informed and if so when
xii. Does the breach indicate a training issue?
xiii. Does the breach indicate an I.T. issue?
xiv. Does the breach require a review of internal processes?
xv. Have the previous 3 points been taken into account when applying step 'x' above?

17.3. The data controller must also complete the GDPR Breach Register, as a permanent record of the breach and the ensuing process followed, even where the breach is minor or suspected.

18. Reporting a breach to the ICO

18.1. When a personal data breach has occurred, the data controller will need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, then they must notify the ICO; if it's unlikely then there is no requirement to report it. However, if it is decided that there is no need to report the breach, the data controller will need to be able to justify this decision, thus it should be should documented.

18.2. In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals, such as:

- loss of control over their personal data or limitation of their rights,
- discrimination,
- identity theft or fraud,
- financial loss,
- unauthorised reversal of previously anonymised data (pseudonymisation),
- damage to reputation,
- loss of confidentiality of personal data protected by professional secrecy or;
- any other significant economic or social disadvantage to the person concerned.

18.3. Please remember, you only have **72 hours** to notify the ICO from when you become aware of the breach.

18.4. If your investigation has not been completed by the time 72 hours is due to elapse, you must still report the breach when you become aware of it and submit further information as soon as possible. If you know you won't be able to provide full details within 72 hours, it is a good idea to explain the delay to the ICO and telling them when you expect to submit more information.

18.5. To report breaches to the ICO, please go to the following website and complete the official forms:

https://ico.org.uk/for-organisations/report-a-breach/

18.6. The following two checklists are to be utilised to help you to prepare for and respond to personal data breaches:

Preparing for a personal data breach

☐ We know how to recognise a personal data breach.

☐ We understand that a personal data breach isn't only about loss or theft of personal data.

☐ We have prepared a response plan for addressing any personal data breaches that occur.

☐ We have allocated responsibility for managing breaches to a dedicated person or team.

☐ Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

Responding to a personal data breach

☐ We have in place a process to assess the likely risk to individuals as a result of a breach.

☐ We know who is the relevant supervisory authority for our processing activities.

☐ We have a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.

☐ We know what information we must give the ICO about a breach.

☐ We have a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms.

☐ We know we must inform affected individuals without undue delay.

☐ We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.

☐ We document all breaches, even if they don't all need to be reported.

19. Reporting a breach to Individuals

19.1. If a breach is likely to result in a 'high risk' to the rights and freedoms of individuals, the GDPR says organisations must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.

19.2. A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. Again, you will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again, the risk is higher. In such cases, you will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them.

19.3. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

19.4. You must describe, in clear and plain language, the nature of the personal data breach and at least:

- the name and contact details of your data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- 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.

20. CLEAR DESK & SCREEN

"We at **The Grenfell Club** operate a Clear Desk & Screen Policy"

20.1. Purpose

20.1.1. The main reasons we have introduced this policy are as follows:

Personal Data, like other important corporate assets, has value and consequently needs to be suitably protected.

Personal Data, in whatever form it takes, or means by which it is shared or stored, should always be appropriately protected. Personal Data security is characterised as the preservation of:

- Confidentiality: ensuring that information is accessible only to these authorised to have access;
- Integrity: safeguarding the accuracy and completeness of information and processing methods;
- Availability: ensuring that authorised users have access to information when required.
- Confidentiality, integrity and availability of information are essential to maintain legal compliance.
- In addition to the aforementioned the following reasons also apply:
  i. It shows the right image when people visit the Charity.
  ii. It reduces the threat of security as passwords and confidential information get locked away.
  iii. Studies have shown a reduction in workplace accidents and spills.

20.1.2. **Policy Statement**

20.1.2.1. To improve the security and confidentiality of information, wherever possible, The Grenfell Club shall adopt a **clear desk policy** for papers and removable storage media and **clear screen policy** for information processing facilities. This is to reduce the risk of unauthorised access, loss of, and damage to information during and outside normal working hours or when areas are unattended.

20.1.3. **Scope**

20.1.3.1. This policy applies to **all** permanent, temporary or contracted employees, volunteers and trustees at The Grenfell Club who access information electronically or otherwise on-site at the Office.

20.1.4. **Principles**

20.1.4.1. The governing principles are detailed below and are to ensure:

- That confidentiality is maintained at all times;
- That all legal requirements are met;
- Compliance with the requirements set out in the following section.

20.1.5. **Legislative requirements**

- For the purpose of this document, and supporting The Grenfell Club ' aim to ensure that all confidential information will be handled sensitively and confidentially, the leading legislative requirements are defined in:
- The GDPR 2018
- Common Law

20.1.6. **Monitoring Arrangements**

20.1.6.1. All staff are responsible for monitoring their compliance with the principles/procedures detailed in this policy; managers should also monitor compliance on a regular basis.

However, we do not expect the policy to be implemented in a heavy-handed way, but we expect that most employees, volunteers and trustees will live with the spirit of the policy. We expect line managers to deal in a sympathetic way with employees, volunteers and trustees.

Although managers are responsible for ensuring that employees, volunteers and trustees clearly understand and adhere to this policy, ultimately it is the responsibility of **all** employees, volunteers and trustees to adhere to the policy's principles and procedures to help maintain the security and confidentiality of information.

20.1.7. **Clear Desk**

20.1.7.1. Firstly, this policy does not preclude individuals personalising their own workspace, so long as this is tastefully done, does not clutter and leaves sufficient working area on your desk.

20.1.7.2. Where practically possible, paper and computer media should be stored in suitable locked safes, cabinets or other forms of secure furniture when not in use, especially outside working hours.

20.1.7.3. All sensitive information should be removed from the work place and stored in a locked area. This includes all customer or supplier-identifiable information, as well as Charity critical information such as salaries and contracts.

20.1.7.4. Sensitive or classified information, when printed, should be cleared from printers immediately.

20.1.7.5. It is good practice to secure all office areas when they are not in use.

20.1.7.6. The reception desk can be particularly vulnerable to visitors. This area should be kept as clear as possible at all times; in particular customer records or employee information should not be held within reach/sight of visitors.

20.1.7.7. It is also worth noting that information left on desks is also more likely to be damaged or destroyed in a disaster such as fire, flood or explosion.

20.1.8. Reduction in the use of paper:

The policy is also designed to help reduce the amount of paper that is used in the Charity, as well as costly toners and inks - particularly from the colour printers. It will also reduce the amount of filing space that we will have to use.

Many people use print offs as a form of backup against losing information from the computer systems. Please rest assured that our IT support backs up all information on a regular basis.

20.1.9. Tips for having a clear desk

i. Put a date and time in your calendar/diary to clear your paperwork
ii. If in doubt - throw it out. If you are unsure of whether a piece of paper should be kept, ask first then discard or destroy if not required.
iii. Do not print off emails solely to read them. This just generates increased amounts of clutter.
iv. Go through the things on your desk to make sure you need them and what you don't need dispose of in the appropriate manner.
v. Handle any piece of paper only once - act on it, file it, shred it, or put it in the bin.
vi. Always clear your desktop before you go home
vii. Consider scanning paper items and filing them in your PC

20.1.10. **Clear Screen**

20.1.10.1. The Grenfell Club Laptops/computer terminals should not be left logged on when unattended and should be password protected.

20.1.10.2. Computer screens should be angled away from the view of unauthorised persons.

20.1.10.3. The Windows Screensaver should be set to activate when there is no activity for a short pre-determined period of time.

20.1.10.4. The Windows Screensaver should be password protected for reactivation.

20.1.10.5. Users should log off their machines when they leave the room, even if only for a short period of time.

20.1.11. It will never be possible for ALL people to maintain a clear desk while working, owing to the nature of certain roles within the Charity. We can ALL however look after security and confidentiality while we work by adopting most if not all of the principles as laid out above and remembering that…

"at the end of the working day staff are expected to tidy their desk and to tidy away all office papers. We provide an under-desk locker and filing storage for this purpose"

APPENDIX 1.

PERSONAL DATA CONSENT FORM

I hereby fully consent to the collection, storage and use of my personal data, which is freely submitted, for the following purpose only:

(* delete as appropriate)

- Care obligations/ Contractual and Legal obligations* / Processing employees' payments*, or as agreed with The Grenfell Club on this day ……

i. I understand that I may withdraw my consent at any time by requesting that withdrawal to this office in writing, or via email to …….. and that my request will be acted upon within one month of my making such a request.

ii. I understand and agree that third party organisations may receive my data and that The Grenfell Club will only submit required personal data for the purpose of _____* / _____* / _____* / _____*.

_____* / _____* / _____*.

iii. I understand that The Grenfell Club shall inform me of any third parties (as stated above), that may process my information prior to submitting that data and that the charity will not submit my data without first obtaining my consent.

iv. I have read and understood the Privacy Notice* and Terms and Conditions regarding the obtaining, storage and processing of my personal data.

Signed: …… Date: ……

Print Name: ……

APPENDIX 2.

DATA SUBJECT ACCESS REQUEST FORM

Please complete this form if you wish to apply for access to your personal data that is held by The Grenfell Club, completing one form for each individual requesting access to data.

N.B.: Completion of this form is not mandatory – Data Subject Access Requests made in other formats are also acceptable, however completion of this form should enable us to prioritise the request.

Data Subject Access Request Guidance Notes

Please read before filling in the Data Subject Access Request Form

Please complete all sections of the form

What information does The Grenfell Club hold?

The Grenfell Club holds data of individuals and all such data may include some or all of the following:

- Name
- Address
- Telephone Number
- Bank Details
- Email Addresses
- Mobile Numbers
- Passport or Driving License for ID purposes*

Why do we hold such information?

Reasons for holding this data include the following:

- Maintaining Client contact
- Invoicing
- Contractual & legal obligations
- Employee processing

How long will it take to get my data?

Once we are satisfied that your request meets the criteria for disclosure of data under the GDPR you will receive a response from us within 30 days from the date of receipt of your application at our offices.

The form includes a section for providing details should you require disclosure by a specific date. No guarantee can be given that a disclosure will be completed by that date, but we shall endeavour to comply with all reasonable requests for expedited action.

General Notes

1. We will not acknowledge your application in writing, but we will provide you with a reference number when we write to you.
2. A fee is not chargeable unless the request for data access becomes manifestly unfounded or excessive. Where the latter conditions exist a fee of £10 may be charged for disclosure.
3. The documents that you receive may have data redacted (blacked-out) or contain rough notes that may lack clarity. This is because we aim to supply copies of the original records whenever possible. However, as some records also include third party information that we cannot release to you under the GDPR, e.g. another person's data, this is removed.
4. Subject Access Requests may sometimes be made on behalf of an of the individual by a representative, only with explicit consent, or power of attorney and where clear consent has been given by the Data Subject.
5. We will not disclose information by text, email or telephone. Disclosure by post is usually made first class post to the address you provide in section 2 or, if appropriate, to your representative named in section 6.
6. **N.B. All access requests made by the police or other governmental authorities will be complied with irrespective of any objections by the Data Subject.**

Checklist

- Have you completed all relevant sections of the form?
- If you are a representative, has your client signed the authority in Section 8 or provided a separate signed note of authority?
- If you are submitting the form yourself, have you signed the form at Section5?
- Have you enclosed two pieces of identification from the lists in Section 3 (one from each of A and B)?
- Have you paid the fee of £10 per SAR (if you have been notified that this is applicable)?
- Have you signed the declaration in Section 5?
- Have you provided as much information as possible to enable us to find the data you require?

Please send your completed form to:

The Grenfell Club
Grant St,
Redcar
TS10 1RW
Email: samantha@grenfellclub.org

The Grenfell Club
inspiring lives

Section 1 – Applicant Details

Title (please tick one):	Mr ☐ Mrs ☐ Miss ☐ Ms ☐ Title (please state):
Forename(s):	
Family Name:	
Previous Family Name:	
Other name(s) known by:	
Date of Birth (dd/mm/yyyy):	……../……./……. Male ☐ or Female ☐
Reference Number:	Reference: ……
Any other information by which we may identify you:	

Section 2 – Applicant Details

Current Address:	
Postcode	
Daytime Telephone No:	
Email Address:	
Previous Address:	
Postcode:	

The Grenfell Club
inspiring lives

Section 3 – Proof of the applicant's identity

In order to prove the applicant's identity, we need to see copies of two pieces of identification, one from list A and one from list B below. Please tick the relevant box to indicate which ones you are supplying.

Please DO NOT send an original passport, driving licence or identity card

List A (photocopy of one from below)		List B (plus one original from below) *	
Passport/Travel Document	☐	A letter sent to you by the Passport Office	☐
Photo driving licence	☐	Utility bill showing current home address	☐
Foreign National Identity Card	☐	Bank statement or Building Society Book	☐

* Any original documents you send to us will be returned by first class post.

Section 4 – Details of Information Required

Please use this space to give us any details about the information you are requesting, for example by stating specific documents you require (use extra sheets if necessary):

Section 5 – Declaration

The information which I have supplied in this application is correct, and I am the person to whom it relates or a representative acting on his/her behalf. I understand that The Grenfell Club may need to obtain further information from me/my representative in order to comply with this request.

Signature of Applicant:	Date:

The Grenfell Club
inspiring lives

Section 6 – Representative Details (if applicable)

(If completed The Grenfell Club will reply to the address that you have provided in this section)

Name of Representative:	
Charity Name:	
Address & Postcode:	
Daytime Telephone No:	
Email Address:	

Section 7 – Proof of the Representative's identity

Please provide copies of two pieces of identification, one from list A and one from list B below and tick the relevant box to indicate which ones you are supplying.

Please DO NOT send an original passport, driving licence or identity card

List A (photocopy of one from below)		**List B (plus one original from below)**	
Passport/Travel Document	☐	**A letter sent to you by the Passport Office**	☐
Photo driving licence	☐	**Utility bill showing current home address**	☐
Foreign National Identity Card	☐	**Bank statement or Building Society Book**	☐

Section 8 – Authority to release information to a Representative

A representative needs to obtain authority from the applicant before personal data can be released. The representative should obtain the applicant's signature below, or provide a separate note of authority.

This must be an original signature, not a photocopy (tip: using blue ink often helps verification).

If the applicant is signing as the guardian of a child under 12, proof of legal guardianship must also be provided.

I hereby give my consent for the representative named in Section 6 of this form to make a Subject Access Request on my behalf under the GDPR.	
Signature of Applicant:	**Date:**
Signature of Representative:	**Date:**

Section 9 – Request for early release of data.

If you have specific reasons for requiring data by a specific date please give details below:

DATE THE DATA IS REQUIRED:
PLEASE STATE YOUR REASON(S) AND ATTACH SUPPORTING EVIDENCE TO THIS FORM: