1st Creigiau Scout Group
(Registered Charity No.1068401)

Data Policy (Version 18.2)

1. Introduction

The 1st Creigiau Scout Group's Executive Committee is responsible for the security, integrity and confidentiality of all the data the Group holds. The Executive Committee is also obliged under GDPR to ensure personal data is safe and secure and respond promptly and appropriately to any data security breaches. Although all adult volunteers have a responsibility for the information they generate, manage, transmit and use in line with GDPR, it is the Executive Committee's legal duty to secure personal and confidential data always.

Any person who knows or suspects that a breach of data security has occurred should report the breach immediately to the Group's Data Protection Officer. One member of the Exec will always be the nominated Data Protection Officer.

Within the Group, the Data Protection Officer will carry out the following tasks:

- Issue advice and information on how the Group needs to comply with the Data Protection laws, including GDPR.
- Monitor compliance against the Data Protection Laws and GDPR and advise on the key documentation to be completed to demonstrate compliance such as the Data Privacy Impact Assessment (DPIA).
- Act as the first point of contact for any supervisory authority, employee or ANY individual or member whose data is being processed, for e.g. donors, supporters and volunteers.

It is vital that prompt action is taken by the Group's Data Protection Officer and Exec Committee in the event of any actual, potential or suspected breaches of data security or confidentiality to avoid the risk of harm to young people or adult volunteers, damage to Group operations and severe financial, legal and reputational costs to the Movement as a whole.

The Group will always, on request, provide a justified reason behind any aspect of its Data Policy. When required, this policy will be updated by the Group's Executive Committee.

2. Data

As part of scouting, Sensitive Personal Data (also known as special category data) is gathered, processed and transferred frequently by the Group. For example:

- New joiner details, be that Adult Volunteer or a Young Person.
- Processing of this data for the purposes of events, awards, moving on.
- Annual reviews of this data through census or further data gathering to update medical records.
- Management of safeguarding incidents where data needs to be transferred to 3rd parties for assistance.

	Young Members	Adult Volunteers
What data /information does the Group Collect?	Collected according to the contents of the current version of the Group's Parental Declaration Document (PDD) form. Some data transferred onto the Online Scout Manager platform.	Collected initially via the Scout Association's New Adult Volunteer forms, Data transferred onto Compass – the Scout Association's central electronic adult volunteer information system.
Why is this data collected?	Personal details and medical records are necessary for the protection of that Young Person whilst in the care of the Scout Group. The collection of Young People's religion is necessary to respect their beliefs with regards to activities, food and holidays.	Adult Volunteers data is necessary for the purposes of disclosure checks, safeguarding and on-going training.

How are the Group collecting the data and how are we using it?	Completion of the PDD form by the parents / guardians on child joining the group	Completion of Adult volunteer form by new volunteers
When will the Group delete the data it holds?	The Group retains the data within the PDD indefinitely for the following reasons: • In case the young person wants to return and continue. • Gift aid data retained for 7 years to meet audit requirements by HMRC. • To prove on-going/retrospective proof of the permissions granted within.	On ceasing to be involved with the Group for whatever reason the data is immediately deleted.
Who can access the data we hold?	Section Leaders of the Section the Young Person is attending, Treasurer, GSL Data Protection Officer (if not one of the above).	GSL Data Protection Officer (if not the GSL).
Where do we store the data we have?	Current & Past PDD forms are stored within the Treasurer's House. Copies are held securely by the relevant section leaders. Data within online scout manager is stored within the Online Scout Manger web platform with restricted access as stated above. Scout Section Leaders store photos in a troop leadership cloud accessible only to warranted leaders.	Data within Compass is stored within the Compass web platform

* All data within the Online Scout Manager platform is either transferred onto the Explorer Scout Leader of the Celts Explorer Scouts on joining of the section, or is securely deleted immediately if they leave the group at any other time.

3. Process for giving Notice of a Personal Data Breach

In the event of a data breach, the Group's Data Protection Officer should receive the following information:

4. Procedure for managing data security breaches

In line with best practice, as recommended by the Scout Association these five steps should be followed when responding to a data security breach:

Step 1: Identification and initial assessment

Step 2: Containment and recovery

Step 3: Risk assessment

Step 4: Notification

Step 5: Evaluation and response

Step 1: Identification and initial assessment of the incident

If the Breach Notification Form (Appendix 1) has not already been completed by the individual reporting the breach, it should be completed as part of this process. The Breach Notification Form will help the Executive Committee to conduct an initial assessment of the incident by establishing if a personal data security breach has taken place, and if so:

- what personal data is involved in the breach
- the cause of the breach
- the extent of the breach, i.e. how many individuals are affected
- the harms to affected individuals that could potentially be caused by the breach
- how the breach can be contained

The Executive Committee will determine the severity of the incident using the reference table on the next page and by completing the Data Breach Severity Form (Appendix 2) (i.e. to decide if the incident can be managed and controlled locally or if it is necessary to escalate the incident to the Information Commissioner's Office (ICO). The severity of the incident will be categorised on a scale of 0 to 6. An extraordinary meeting of the Exec will be called by the Data Protection Officer in the event of the most serious data breaches?

Rating	0	1	2	3	4	5	6
Reputation	No significant reflection on any individual or body Media interest very unlikely.	Damage to an individual's reputation. Possible media interest (e.g. prominent member of the Charity involved).	Damage to a Scout Group, District, Area's reputation. Some local or national subject specific media interest that may not go public.	Damage to the Charity's reputation. Low key local or national media coverage.	Damage to The Scout Association's reputation. Local media coverage.	Damage to The Scout Association. National media coverage.	Monetary penalty Imposed by ICO.
Clients potentially affected	Minor breach of confidentiality. Only a single individual affected.	Potentially serious breach. Less than five individuals affected, or risk assessed as low (e.g. files were encrypted).	Serious potential breach and risk assessed high (e.g. unencrypted sensitive/health records lost) Up to 20 individuals affected.	Serious breach of confidentiality e.g. up to 100 individuals affected and/or identifiable or particularly sensitive ie redundancies/restructuring.	Serious breach with either a particular sensitivity (e.g. sexual or mental health details, or up to 1000 individuals affected.	Serious breach with potential for ID theft or over 1000 individuals affected.	Restitution to injured parties. Other Liabilities. Additional security. Legal costs.
Communications	Maintain internal communications to members.	Maintain internal communications to the members.	Maintain internal communications to the members. Also inform the individuals affected as well as the ICO.	Maintain internal communications to the members. Also inform the individuals affected as well as the ICO.	Maintain internal communications to the members. Also inform the individuals affected as well as the ICO.	Maintain internal communications to the members. Also inform the individuals affected as well as the ICO.	Maintain internal communications to the members. Also inform the individuals affected as well as the ICO.

Step 2: Containment and Recovery

Once it has been established that a data breach has occurred, the Executive Committee needs to take immediate and appropriate action to limit the breach.

The Executive Committee will:

- Establish who within the Scout Group, District, Area needs to be made aware of the breach and inform them of what they are expected to do to contain the breach (for example finding a lost piece of equipment, changing access codes on doors, isolating/closing a compromised section of the network, etc)
- Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause (for example physical recovery of equipment/records, the use of back-ups to restore lost/damaged data)
- Establish if it is appropriate to notify affected individuals immediately (for example where there is a high level of risk of serious harm to individuals)
- Where appropriate (for example in cases involving theft or other criminal activity), inform the police.

Step 3: Risk Assessment

In assessing the risk arising from a data security breach, the Executive Committee are required to consider the potential adverse consequences for individuals, i.e. how likely are adverse consequences to materialise and, if so, how serious or substantial are they likely to be. The information provided on the Breach Notification Form will help with this stage.

The Executive Committee will review the incident report to:

- Assess the risks and consequences of the breach.
- Risks for individuals.
- What are the potential adverse consequences for individuals?
- How serious or substantial are these consequences?
- How likely are they to happen?
- Risks for the Charity / Trust.
- Strategic and operational.

- Compliance/legal.
- Financial.
- Reputational.
- Consider what type of data is involved, how sensitive is it? Were there any protections such as encryption? What has happened to the data? If data has been stolen it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged this poses a different type and level of risk.
- Consider how many individuals' personal data are affected by the breach. It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment.
- Consider the individuals whose data has been breached. Whether they are young people or adult volunteers will to some extent determine the level of risk posed by the breach and therefore, the actions in attempting to mitigate those risks.
- Consider what harm can come to the affected individuals. Are there risks of physical safety or reputation, of financial loss or a combination?
- Consider if there are wider consequences to consider such as a loss of public confidence in Scouting as a whole.
- Determine, where appropriate, what further remedial action should be taken on the basis of the incident report to mitigate the impact of the breach and prevent repetition.

The Executive Committee will prepare an **incident report** setting out (where applicable):

- a summary of the security breach
- the people involved in the security breach (such as young people, adult volunteers)
- details of the information, IT systems, equipment or devices involved in the security breach and any information lost or compromised as a result of the incident
- how the breach occurred
- actions taken to resolve the breach
- impact of the security breach
- unrealised, potential consequences of the security breach
- possible courses of action to prevent a repetition of the security breach
- side effects, if any, of those courses of action
- recommendations for future actions and improvements in data protection as relevant to the incident

The incident report will then be used to update the risk registers at the appropriate levels where necessary. Any significant risks will be reported and managed via the Risk Register in the GDPR Framework.

Step 4: Notification

On the basis of the evaluation of risks and consequences the Executive Committee, and others involved in the incident as appropriate, will determine whether it is necessary to notify the breach to others outside the Scout Group, District or Area. For example:

- parents
- individuals (data subjects) affected by the breach
- the Information Commissioner's Office
- police
- the press/media via The Scout Association's Headquarters media team
- Trust / Charity insurers
- bank or credit card companies
- external legal advisers

As well as deciding **who** to notify, the Executive Committee must consider:

- **What** is the message that needs to be communicated?
  In each case, the notification should include as a minimum:
  - a description of how and when the breach occurred;
  - what data was involved; and
  - what action has been taken to respond to the risks posed by the breach.

  When notifying individuals, the Executive Committee should give specific and clear advice on what steps they can take to protect themselves, what the Scout Group, District, Area on is willing to do to assist them and details of how they can contact the Executive Committee for further information.
- **How to communicate the message?**

  What is the most appropriate method of notification (for example are there large numbers of people involved? Does the breach involve sensitive data? Is it necessary to write to each individual affected? Is it necessary to seek legal advice on the wording of the communication?)

- **Why are we notifying?**

  Notification should have a clear purpose, for example to enable individuals who may have been affected to take steps to protect themselves (e.g. by cancelling a credit card or changing a password), to allow regulatory bodies to perform their functions, provide advice and deal with complaints, etc

Although there is no legal requirement on the Executive Committee to report breaches of security which result in loss, release or corruption of personal data, the Information Commissioner's Office (ICO) expects that serious breaches should be brought to their attention. Serious breaches are not defined but guidance is available on the ICO website under Data Protection principle 7 Data Security.

Any contact with the ICO should be made by the Data Protection Officer. Initial contact with the ICO should be made by the Executive Committee within **two working days** of becoming aware of the breach, outlining the circumstances surrounding the incident through submission of the Breach Notification Form and the Breach Severity Form. The ICO will make a determination regarding the need for a detailed report and/or subsequent investigation based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data. In cases where the decision is made by the Executive Committee not to report a breach, a brief summary of the incident with an explanation of the basis for not informing the ICO will be retained by the Executive Committee.
When the personal data breach is likely to result in a high risk to the rights and freedoms of those affected, the Executive Committee shall communicate the personal data breach to the data subject without undue delay.

The communication to the data subject referred to in paragraph one shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to above.

The communication to the data subject shall not be required if any of the following conditions are met:

- **The Executive Committee has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption**
- **The Executive Committee has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise**
- **it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner**

If the Executive Committee has not already communicated the personal data breach to the data subject, the ICO, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to are met.

Step 5: Evaluation and Response

Subsequent to a data security breach, the Executive Committee will conduct a review to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

The Executive Committee will compile a central record of incidents in the GDPR Framework. The Executive Committee will report on incidents to the adult volunteers in order to identify lessons to be learned, patterns of incidents and evidence of weakness and exposures that need to be addressed.

For each **serious** incident, the Executive Committee will conduct a review and report:

- what action needs to be taken to reduce the risk of future breaches and minimise their impact
- whether policies procedures or reporting lines need to be improved to increase the effectiveness of the response to the breach
- if there are any weak points in security controls that need to be strengthened
- if users of services are aware of their responsibilities for information security and adequately trained
- if additional investment is required to reduce exposure and if so what are the resource implications?
- if the breach was 'reckless' and of such a serious a consequence that there be a recourse to remove the person/s responsible from the Group

Appendix 1 - Breach Notification Form

NAME, ADDRESS & PREFERRED CONTACT DETAILS	
Date of breach	
Breach description	
Breach effect	
Number of data subjects affected	
Personal data affected	
Number of personal data records affected	
Likely consequences of the breach	
Remedial action taken	
Date of remediation	

SIGNED	
NAME AND TITLE	

Appendix 2 - Data Breach Severity Form

Assessment of severity	To be completed by the Executive Committee
Details of the IT systems, equipment, devices, records involved in the security breach	
Details of information loss	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the organisation or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data o **Sensitive personal data** (as defined in the Data Protection Act) relating to a living, identifiable individual's a) racial or ethnic origin b) political opinions or religious or philosophical beliefs c) membership of a trade union d) physical or mental health or condition or sexual life e) commission or alleged commission of any offence, or f) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings	
o Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as National Insurance Number and copies of passports and visas	
o Personal information relating to vulnerable adults and children	
o Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed	
o Security information that would compromise the safety of individuals if disclosed	
Category of incident (0-6):	
Reported to Executive Committee on:	
If level 2 or above, date escalated by the Executive Committee to the ICO	

Action taken	To be completed by the Executive Committee
Incident number	**e.g. DB/year/001**
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Was incident reported to police?	**Yes/No** **If YES, notified on (date):**
Follow up action required/recommended:	
Reported to the Executive Committee on (date):	
Reported to other internal stakeholders (details, dates):	
For use of the Executive Committee	
Notification to ICO	**YES/NO** **If YES, notified on:** **Details:**
Notification to data subjects	**YES/NO** **If YES, notified on:** **Details:**
Notification to other external, regulator/stakeholder	**YES/NO** **If YES, notified on:** **Details:**