****

**6**

|  |
| --- |
| [insert name of Group] |

Note from Bishop’s Stortford and District Scouting: a *process like this is highly recommended in case of a data breach in your Group.* The broad text is recommended and where there are [ brackets ] you need to insert your relevant Group information. If you have questions email the District Commissioner, Greg here.

**Personal Data Breach Incident Procedures**

**For use by GSL and Group Chair**

It is important that the Group Scout Leader and Group Chair read this procedure and be familiar with what to do if a data breach is reported to them. Under Data Protection Law, all organisations have a duty to report certain types of data breach quickly to the **Information Commissioner’s Office** (ICO) and in some cases to the individuals affected.

**Likely sequence of events**

****

The Group must use appropriate technical and organisational measures to protect the personal data of members and volunteers including protection against *unauthorised or unlawful processing* and against *accidental loss*, *destruction* or *damage*.

For clarity the definitions are:

|  |  |
| --- | --- |
| “*Damage*” | Where personal data has been altered, corrupted, or is no longer complete |
| “*Unauthorised Destruction*”  | Where personal data no longer exists, or no longer exists in a form that is of any use to the Group.  |
| “*Accidental loss*” | Where the data may still exist, but the Group has lost control or access to it, or no longer has it in its possession. |
| “*Unauthorised or unlawful processing*” | Includes disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the Law. |

**What breaches must the Group report to the ICO?**

The Group needs to report a breach where it is likely to result in a *risk to the rights and freedoms of individuals*. If unaddressed, such breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

This will be assessed on a case by case basis. An example would be if the Cub Leader lost a file with the leaders names, addresses and dates of birth. We would have to inform the ICO as this loss could leave individuals open to identity fraud. On the other hand, the loss or inappropriate alteration of a Leaders telephone numbers, for example, would not normally meet this threshold.

**When would the Group have to notify individuals?**

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the Group must notify those concerned directly. A ‘high risk’ means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority. The GSL or Group Chairman, advised by the District will manage this process.

**Informing the ICO**

A notifiable breach **must** to be reported to the ICO within **72 hours** of the Group first becoming aware of it. The law recognises that it will often be impossible to investigate a breach fully within this time-period and allows organisations to provide information in phases. The law goes on to say that if the breach is sufficiently serious to warrant notification to the public, the Group must do so without undue delay. Where a notification to the ICO is not made within 72 hours, it shall be accompanied by reasons for the delay. Failing to notify a breach when required can result in a significant fine. The GSL/Group Chair will manage the communications and liaison with the ICO’s office.

**How will the Group inform the ICO?**

The attached form is to be used (attached for Group Executive information only)

|  |
| --- |
| **REMEMBER**The Information Commissioner’s Office MUST be contacted within **72 Hours** of the first indication of a reportable breach.**When a Leader receives information about any breach, the** [🡺 *insert role (not name) of person responsible for the Group data Protection*]. **must be informed immediately– in this process every hour counts.** |

Date AGREED:

Next REVIEW date

**The** [🡺 *insert role (not name) of person responsible for the Group data Protection*] **will complete this form:** Provide as much information as possible and ensure that all mandatory (\*) fields are completed – you can always go back to the ICO with information at a later stage.

1. **ORGANISATION DETAILS:**

|  |  |  |
| --- | --- | --- |
| \***Our Group is:** |  | [🡺Needs a contact address] |
|  |  |  |
| **\*Who is reporting breach to ICO:** |  |  |
|  |  |  |  |
| **\*Your phone number and email:** |  | Phone: |  |
| Email: |  |
|  |  |  |
| **\*Name of Group contact who should be the contact for the ICO:** |  | [🡺 *insert role (not name) of person responsible for the Group data Protection*]. |
|  |  |  |
| **\*Is the Group responsible for this breach:** |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| YES |  | NO |  | Don’t Know |  |

 |
|  |  |  |
| **\*If NO which third party is responsible?** |  | Name and contact details: |

1. **DETAILS OF THE BREACH**

|  |
| --- |
| 1. **\*Describe the nature of breach with as much detail as possible:**
 |
| **This breach is about:**

|  |  |  |
| --- | --- | --- |
| **The categories of breach** |  | **🗸** |
| **Unauthorised destruction** |  |  |
| **Damage** |  |  |
| **Accidental Loss** |  |  |
| **Unauthorised or unlawful processing** |  |  |

**More details**: |

|  |  |  |
| --- | --- | --- |
| 1. **\*When did the incident happen:**
 |  |  |

|  |
| --- |
| 1. **\*How did the incident happen:**
 |
|  |

|  |
| --- |
| 1. **If there has been a delay in reporting to ICO why is this?**
 |
|  |

|  |
| --- |
| 1. **\*What measures did the Group have in place to prevent an incident of this nature occurring?**
 |
|  |

|  |
| --- |
| **(e) Please provide extracts of any policies and procedures considered relevant to this incident, and**  **explain which of these were in existence at the time this incident occurred. Please provide the dates**  **on which they were implemented.** |
|  |

**3.**  **PERSONAL DATA PLACED AT RISK**

|  |
| --- |
| 1. **\*What personal data has been placed at risk? Please specify if any financial or sensitive personal data**

 **has been affected and provide details of the extent.** |
|

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | **🗸** |  |  |  | **🗸** |  |  |
| **Name** |  |  |  | Date of Birth |  |  |  | **Other Please describe** |
| **Address** |  |  |  | NI Number |  |  |  |  |
| **Phone** |  |  |  | Medical |  |  |  |
| **Email** |  |  |  | Financial |  |  |  |

**Other comments:** |

|  |  |  |
| --- | --- | --- |
| **(b) \*How many individuals are affected?** |  |  |

|  |
| --- |
| **(c)\* Are the affected individuals aware that the incident has occurred?** |
|

|  |  |  |
| --- | --- | --- |
| **Yes** |  |  |
| **No** |  |  |
| **Not sure** |  |  |

 |

|  |
| --- |
| **(d) \*What are the potential consequences and adverse effects on those individuals?** |
|  |

|  |
| --- |
| **(e) Have any affected individuals complained to the organisation about the incident?**  |
|

|  |  |  |
| --- | --- | --- |
| **Yes** |  |  |

|  |  |  |
| --- | --- | --- |
| **No** |  |  |
| **Not sure** |  |  |

 |

**4. CONTAINMENT AND RECOVERY**

|  |
| --- |
| **(a) \* Has the Group taken any action to minimise/mitigate the effect on the affected individuals?** **If so, please provide details.** |
|  |

|  |
| --- |
| 1. **\* Has the data placed at risk now been recovered? If so, please provide details of how and when this**

 **occurred.** |
|  |

|  |
| --- |
| **(c)\* What steps has the Group taken to prevent a recurrence of this incident?**  |
|  |

**5.** **TRAINING AND GUIDANCE**

|  |
| --- |
| 1. **Describe the training on Data Protection Act volunteer receive.**
 |
|  |

|  |
| --- |
| 1. **Does the Group provide any detailed guidance to volunteers on the handling of personal data in relation to the incident being reported? If so, please provide any extracts relevant to this incident here.**
 |
|  |

**6. PREVIOUS CONTACT WITH THE ICO**

|  |
| --- |
| 1. **Have the Group reported any previous incidents to the ICO in the last two years?**
 |
|

|  |  |  |
| --- | --- | --- |
| **Yes** |  |  |

|  |  |  |
| --- | --- | --- |
| **No** |  |  |

**If yes, provide brief details, the date on which the matter was reported and, where known, the ICO reference number.** |

**7. MISCELLANEOUS**

|  |
| --- |
| 1. **Has the Group notified any other (overseas) data protection authorities about this incident? If so, please provide details.**
 |
|  |

|  |
| --- |
| 1. **Has the Group informed the Police about this incident? If so, please provide further details and specify the Force concerned.**
 |
|  |

|  |
| --- |
| 1. **Has the Group informed any other regulatory bodies about this incident? If so, please provide details e.g. Charity Commissioners**
 |
|  |

|  |
| --- |
| 1. **Has there been any media coverage of the incident? If so, provide details of this.**
 |
|  |

|  |  |  |
| --- | --- | --- |
| **Form Completed by:** |  |  |
|  |  |  |
| **Role:** |  |  |
|  |  |  |
| **Date and Time of Completion** |  |  |

Once completed, please telephone the ICO on **0303 123 1113** or **01625 545745** (operates 9am to 5pm Monday to Friday) and send the completed form immediately to:

casework@ico.org.uk with ‘**DPA breach notification form’** in the subject field.

**Next steps**

When the ICO receive this form, they will contact us within seven calendar days to provide:

* a case reference number; and
* information about our next steps.