Cork Deaf Association
DATA BREACH NOTIFICATION POLICY

A) AIM

We are aware of the obligations placed on us by the General Data Protection Regulation (GDPR) in relation to handling data lawfully and making sure that data is kept secure.

One of our obligations is to report a breach of personal data in certain circumstances.
This policy shows how we handle data breaches.

B) PERSONAL DATA BREACH

A personal data breach is a breakdown in personal data security which leads to:

- accidentally or unlawfully destroying personal data which is transmitted, stored or handled.
- Losing personal data which is transmitted, stored or handled.
- Changing personal data which is transmitted, stored or handled.
- Unauthorised disclosure (making private information known to people who should not know) of personal data which is transmitted, stored or handled.
- Accessing personal data which is transmitted, stored or handled.

The following are examples of data breaches:

a) access by a group or person who does not have authority to access the personal data;
b) something which is accidentally or deliberately done or not done by the people controlling or handling the personal data
c) sending personal data to the wrong person;
d) laptops or phones holding personal data being lost or stolen;
e) changing personal data without permission;
f) loss of availability of personal data.

C) WHAT WE DO TO HELP DETECT A PERSONAL DATA BREACH

We do the following things to help us to detect a personal data breach:
- Making sure that we are linked with an IT company who can can help us to understand where and how cyberattacks occur so that proper controls can be put in place.
- Ongoing training to help staff understand how to identify and report early warning signs of an IT attack campaign such as:
  - Unusually slow Internet or devices
  - Locked out accounts
  - Pop-ups and redirected websites when browsing
  - Unexpected software installations
  - Unexplained changes to files
  - Network accessed from unusual locations
  - Large number of requests for the same objects or files
  - Suspicious activity on the network after-hours
  - Multiple failed login attempts
  - Unknown/unauthorized IP addresses on wireless networks
  - Unexplained system reboots or shutdowns

- Services and applications set up to launch automatically

- Ongoing management monitoring of staff data handling, including management spot checks to make sure that all staff are following thee rules of a 'clean desk' policy.

D) INVESTIGATION INTO SUSPECTED BREACH

If we become aware of a breach, or a potential breach, there will be an investigation by a member of the management team. The investigating person will decide if they need to contact the Data Protection Commission to tell them about the breach. They will also decide if the person the breach is about must also be told.

E) WHEN A BREACH WILL BE NOTIFIED TO THE DATA PROTECTION COMMISSIONER

We will notify the Data Protection Commission of a breach which likely to be a risk to people's rights and freedoms.

A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.

We will notify the Data Protection Commission without unnecessary delay and at the latest, within 72 hours of discovering the breach or potential breach. If we are unable to make a full report in this timescale, we will make an initial report to the Information Commissioner and then give a full report in more than one instalment, if required.

The following information will be given when a breach is notified:

a) a description of the kind of personal data breach including, where possible:

   i) the categories of people involved and the approximate number of people involved
   ii) the categories of personal data records involved and approximate number of personal data records involved

b) the name and contact details of the CDA Manager/Deputy Manager where further information can be gotten;
c) a description of the likely consequences of the personal data breach;
d) a description of what was done or what is planned to be done to deal with the personal data breach, including, where appropriate, what was done to reduce the possible harmful effects of the data breach.

F) WHEN A BREACH WILL BE NOTIFIED TO THE INDIVIDUAL

We will notify the individual who is the subject of a breach if there is a *high* risk to people's rights and freedoms.

A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are made known online.

This notification will be made without unnecessary delay. Depending on the circumstances, the individual may be told before the supervisory authority is notified.

The following information will be given when a breach is notified to the affected individuals:

a) a description of the nature of the breach
b) the name and contact details of the CDA Manager/Deputy Manager where further information can be gotten;
c) a description of the likely consequences of the personal data breach and
d) a description of what was done or what is planned to be done to deal with the personal data breach, including, where appropriate, what was done to reduce the possible harmful effects of the data breach.

G) RECORD OF BREACHES

The CDA records all personal data breaches regardless of whether or not they need to be reported. The Record Of Data Breaches records the facts relating to the breach, its effects and what was done to fix the breach.