

10.20 Personal Data Breach

Policy statement

In our setting we have robust procedures in place to detect, investigate and report any personal data breaches. Any member of staff identifying a breach of personal data will report this to our Finance Administrator and/ or Manager to investigate. On occasions where a personal breach of data occurs, the following procedures will be followed:

Personal data breaches can include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a member of staff
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

Breach of Personal data

- We have robust procedures in place to detect, investigate and report any personal data breaches.
- A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- If we experience a personal data breach we will consider whether this poses a risk to people. We will consider the likelihood and severity of the risk to people's rights and freedoms, following the breach.
- When we have made this assessment, we will determine whether the incident is a 'low risk' or 'high risk' breach of personal data. We do not need to report every breach of data to the ICO.

Low Risk Breach of Data:

- Where there is a 'low risk' breach of personal data occurs, details of the instance are investigated and reported. This is not reported to the ICO.
 - The incident is recorded on the GDPR Breach Reporting Register
 - Details of the investigation are recorded on the register
 - Details of the action taken are recorded on the register
 - Where personal data has been disclosed, all parties will be notified.
 - The manager of the setting will sign off the register to confirm appropriate action has been taken
- Where there are a number of 'low risk' breaches occurring for the same reason further, more robust procedures will be implemented to ensure these instances are not repeated. Ongoing occurrences will be reported to the ICO.

High Risk Breach of Data:

- Where the data breach adversely affects ‘people’s rights and freedoms’ and risks causing ‘emotional distress, physical and material damage’ the ICO will be notified within 72 hours of us becoming aware of the personal data breach.
 - The incident is recorded on the GDPR Breach Reporting Register
 - Details of the investigation are recorded on the register
 - The ICO will be contacted on 0303 123 1113 and we will confirm:
 - What has happened
 - When and how we found out about the breach
 - The people that have been or may have been affected by the breach
 - What action we have taken
 - Details of the person the ICO can contact for more information and who has been told of the incident
 - Details of the action taken are recorded on the register
 - Where personal data has been disclosed, all parties will be notified.
 - The manager of the setting will sign off the register to confirm appropriate action has been taken

Telephone advice regarding general queries may be made to The Information Commissioner’s Office Helpline 0303 123 1113.

Legal framework

- General Data Protection Regulations (GDPR) (2018)
- ICO Website: <https://ico.org.uk/for-organisations/report-a-breach/>

Further guidance

This policy was adopted by

Helpston Playhouse

On

30th May 2019

Date to be reviewed

30th May 2020

Signed on behalf of the provider

Name of signatory

Amy Ellis

Role of signatory (e.g. chair, director or owner)

Chair