CHICKENSHED

THEATRE CHANGING LIVES

Chickenshed Data and Security Policy

A breach of the Data Protection Act 2018 could damage Chickenshed's reputation in addition to the Information Commissioner fining the institution for a serious breach. This Policy addresses issues that can protect Chickenshed from issues protection breach.

What constitutes a data protection breach?

A personal data breach involves a breach of security leading to the accidental or unlawful destruction, loss, alteration, un-authorised disclosure of, or access to personal data.

Examples of data breaches include the following (this list not being exhaustive)

- A mobile device (e.g. laptop, mobile phone, memory stick [USB]) or paper files containing personal or sensitive data is lost or stolen
- An unencrypted memory stick is used to store personal or sensitive data in breach of Chickenshed's own policies
- An email or letter containing personal or sensitive data is sent (either internally or externally) to the wrong person(s) or address(es)
- An email or letter is sent (either internally or externally) containing personal or sensitive data which is far in excess of that necessary in order for the business function to be carried out
- An email is sent (either internally or externally) which should be sent "Bcc" to a large number of individuals, is instead, sent "to" and so the recipient is aware who else has received the email and their personal email address or other personal details
- A breach or unauthorized access into a Chickenshed system that holds personal or sensitive information
- Personal or sensitive data is shared outside of Chickenshed for a legitimate business reason, but it is lost by the recipient, or it is stolen from the recipient, or it is used by the recipient in a manner for which they have no authority for
- Paper files of personal data are left unattended and are taken or copied and then used for an unauthorised purpose
- A member of staff uses personal or sensitive data for a personal rather than

- The accidental deletion of records containing personal information
- Alteration of personal data without permission

How should a data breach be reported?

Immediate action must be taken to report the data breach to the Executive and the IT Director. This report should include the following information:

- The circumstances surrounding how the breach occurred
- The extent of the breach
- The implications of the breach
- The actions which have been taken/are needed to be taken to contain/minimise/remedy the breach
- Actions to ensure processes are amended to prevent future occurrence of the breach

An internal investigation will take place under the oversite of the IT Director and any consultants during which the internal Data Security Breach Notification form will be completed. The Director will then determine, in consultation with the Executive Leadership Team, as to whether the breach should be notified to the individuals affected (if they have not already been advised) and/or to the Information Commissioners Office.

Consideration will be given to:

- Whether the breach is likely to result in a high risk to the rights and freedoms of individuals
- The number of individuals who have been affected by the breach
- The sensitivity of the data lost/released/unlawfully corrupted
- The severity of the potential consequences
- Any legal or contractual requirements
- Advisory documentation produced by the Information Commissioners Office

A record of breaches will be maintained centrally, and the Chickenshed Leadership Group will receive a summary of all such breaches on an annual basis.

CHICKENSHED

THEATRE CHANGING LIVES

How to avoid a data breach

- Process data in accordance with Chickenshed's Data Protection Policy
- Undertake the mandatory data protection and cyber security training required by the Chickenshed
- Carefully check email recipients before sending an email
- Use 'Bcc' in cases where recipients are unlikely to know each other and/or personal email addresses are being used
- Lock your computer when away from your desk
- Maintain a clear desk
- Ensure that any documents containing personal information are locked away and not left unattended
- Take care not to talk about personal matters where you could be overheard, or tell a person something that they are not entitled to know
- Seek advice from the IT Director before responding to external requests for personal information.