Cambridge & Ely
Child Contact Centre

Phone: +44 7812 157448
Email: mary@ceccc.org.uk

Registered Charity Number: 1145344
Company Registration Number: 7464402

Security Incident Policy

Introduction

Cambridge & Ely Child Contact Centres will manage any security incidents. This procedure details the actions and roles required when a security incident occurs. It is provided as guidance to staff. All security incidents are recorded. A security incident are issues that potentially impact on the confidentiality, integrity or availability of the centres systems or services.

Procedure

Security incidents will be reported to Mary Parker, Co-Ordinator.

On receipt of the security incident report Mary Parker will take the following actions

i. notification that an incident has occurred from a member of staff or family e.g., stolen laptop, or complaint.

ii. Confirm the type of incident and gather any additional information required by the ICO.

iii. Log the incident including a brief description, time, and date of the incident, who notified the incident and assign a priority High, Medium or Low.

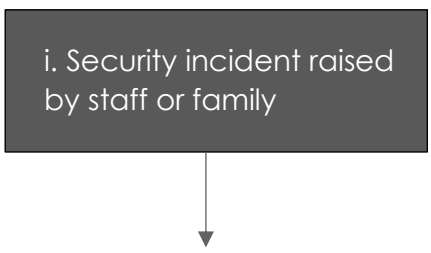
iv. Investigate the incident.

v. Diagnose the incident and identify any actions required to resolve the incident see Incident Types and Responses. Where necessary escalate to ICO as soon as possible and within 72hrs. Notify any affected individuals.

vi. Incident Resolved -update incident record with details of actions taken and results of any investigation regarding the cause whether this was human error or a systemic issue.

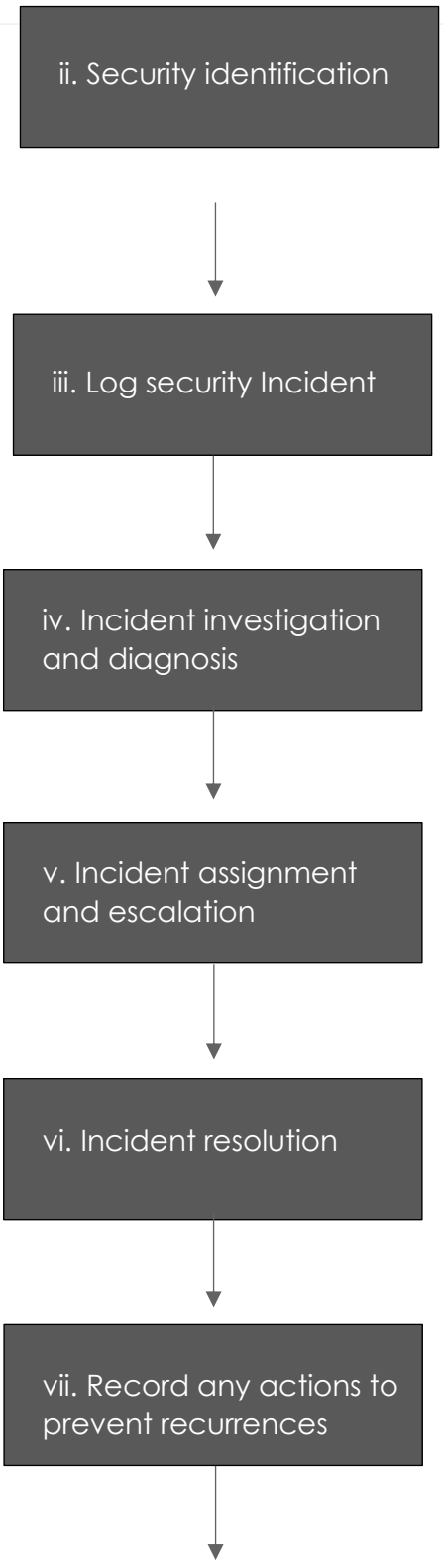
vii. Record any details of how recurrence can be prevented – whether this is through better processes, further training, or other corrective steps.

viii. Close incident.



Phone: +44 7812 157448
Email: mary@ceccc.org.uk

Registered Charity Number: 1145344
Company Registration Number: 7464402



Phone: +44 7812 157448
Email: mary@ceccc.org.uk

Registered Charity Number: 1145344
Company Registration Number: 7464402

viii. Close incident

Responses

Personal Data Leakage Response

If the incident results in the loss of personal data as defined in the DPS (2018) / GDPR then it must be reported to the ICO.

Examples of a data breach personal data breaches can include:

- access by an unauthorised third party.
- deliberate or accidental action (or inaction) by a controller or processor.
- sending personal data to an incorrect recipient.
- computing devices containing personal data being lost or stolen.
- alteration of personal data without permission; and
- loss of availability of personal data.

Under the GDPR there is a requirement for organisations to report a personal data breach that affects people's rights and freedoms, without undue delay and, where feasible, not later than 72 hours after having become aware of it. Organisations should be aware that the ICO will have the ability to issue fines for failing to notify and failing to notify in time. Fines can be avoided if organisations are open and honest and report without undue delay, which works alongside the basic transparency principles of the GDPR.

Serious breaches should be reported to the ICO using our DPA security breach helpline on 0303 123 1113 (open Monday to Friday, 9am to 5pm). Select option 3 to speak to staff who will record the breach and give you advice about what to do next.

Further information can be found at.

https://ico.org.uk/for-organisations/report-a-breach/

Criminal Attack Response

If the incident is a potential attack incident, the incident will be reviewed and if an attack is confirmed it should be reported as such to the customer who will report it to the relevant law enforcement body. The Cambridge & Ely Child Contact Centres will zip and sign the relevant evidence, collected from logs etc. earlier. This evidence will be made available to the customer

Phone: +44 7812 157448
Email: mary@ceccc.org.uk

Registered Charity Number: 1145344
Company Registration Number: 7464402

as required, subject to confidentiality undertakings (it will contain non-customer specific sensitive information). The complete pack will be preserved for subsequent law enforcement action.

Denial of Service (DoS) Response

This has become an increasing threat recently, often manifested as a distributed denial of service (DDoS) attack, which is more difficult to combat. Access to botnets is becoming increasingly widespread so that individuals with grievances have access to facilities hitherto only available to criminal organisations. The attack could be directed at Cambridge & Ely Child Contact Centres could be subject to collateral damage due to attacks on adjacent services. DoS and particularly DDoS attacks can result in:

- The Cambridge & Ely Child Contact Centres web site being unable to respond to legitimate transactions as they are swamped by a flood attack. This would be a direct attack from a low-capacity resource.
- The hosting site being forced to suspend the service to enable other services on their site to continue. If this is a direct attack, Cambridge & Ely Child Contact Centres would be suspended, if Cambridge & Ely Child Contact Centres was suffering collateral damage this would re-open the Contact Centre.
- The ISP switching off access to the v to prevent their service from being overwhelmed. Again, if this is a direct attack, Cambridge & Ely Child Contact Centres would be suspended, if Cambridge & Ely Child Contact Centres was suffering collateral damage this would re-open Cambridge & Ely Child Contact Centres.

For a DoS attack or low-capacity DDoS, action from the hosting provider to block traffic from specific incoming IP addresses should be taken. Arrangements for this action will be made with each hosting site.

For DDoS, the customer should be contacted and, subject to their agreement Emergency DDoS protection should be put in place. As this is chargeable, the customer's agreement and order must be obtained before invoking the service.

The Cambridge & Ely Child Contact Centres will maintain a list of suitable service providers, contact details and costs.

Malware Discovery

Where malware is discovered by routine application of anti-malware measures, this should be logged.

Web Exploit

In most cases, this will be a new exploit. We need to cover, routinely, the OWASP exploits refer to: http://www.ibm.com/developerworks/library/se-owasptop10/index.html, although some variants may need modified responses. On discovery of a web exploit, we will put devise and put into place an emergency fix / procedure to block the exploit. We will check against the OWASP

Phone: +44 7812 157448
Email: mary@ceccc.org.uk

Registered Charity Number: 1145344
Company Registration Number: 7464402

list if the exploit is known. If it is not, we will inform OWASP of the exploit, providing details as required. If it is a deliberate act, we will invoke our Criminal Attack Response, including the session logs in our evidence pack.

Definitions

Incidents will be classified according to their impact on the Cambridge & Ely Child Contact Centres systems or services.

Level	Impact
High	Actual breach effecting the availability, integrity or confidentiality of the Cambridge & Ely Child Contact Centres critical information assets.
Medium	Vulnerability discovered which, if exploited could give rise to a data breach.
Low	Other types of security incident.

ICO data required

A description of the nature of the personal data breach including, where possible:

- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned.
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained.
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Implementation

Reviewed by		
Name Bridget Giltinane	Signature: B.Giltinane	Date: 03.06.2026
This Policy will be reviewed no less than once every three years.		