ANDERIDA ADOLESCENT CARE

CYBER SECURITY AND DATA BREACH POLICY

Our company cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure. The more we rely on technology to collect, store, and manage information, the more vulnerable we become too severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation.

Anderida Adolescent Care has taken all correct measures possible to ensure our company, children, Employees, and visitors are secure. As we are a small organisation, we have had to take additional measures to secure ourselves by outsourcing and investing in a strong IT organisation to manage our Cyber Security and placing all staff through training.

We have implemented a number of security measures such as a Vulnerability Assessment that is completed Bi-annual. Focus Group Scan the network entry point from the outside to see if there are ways a criminal could exploit to gain access to the internal network through the security system. The company domain is scanned through Dark Web Monitoring 24/7 to ensure we can act in a timely manner if any breaches may occur.

REQUIREMENTS

With all the specific requirements that Anderida has put in place to protect our environment we expect every employee to contribute to help keep us remain secure.

PASSWORDS

- Choose strong passwords for all devices within the homes and/or organisation, email and server passwords provided by focus group should not be changed without discussion with the DPO (Anderida's Data Protection Officer is Jane Bettley). In cases where passwords are changed, it is strongly advised that the following guidance is used to ensure security- https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0
- Keep passwords confidential
- Never re-use a password
- Never allow anyone outside the organisation access to the company's systems using your log in details

DEVICES

- You must not turn off or remove any security measures i.e. anti-virus software, firewalls, web filtering, encryption or automatic updates that Focus Group have installed on your computer, phone or network.
- You must not install software onto a company computer or phone, if you have a software request this should be made to the Head Office.
- You must not store any banking details of the organisation on your computer or phone.

EMAIL SAFETY – If you suspect that an email could be a scam:

Anderida have invested in office 365 Advanced threat protection. These are policies that are used to protect the organisation. All staff with an office 365 account provided to them by Focus Group, these accounts are monitored and protected with the below policies.

- **Anti-Phishing** – This policy protects users from Phishing attacks which are commonly known as emails sent impersonating a user of high standing in the business such as the CEO, Managers, or Financial Staff, etc. Any emails found in breach of this policy will be marked as junk automatically by Focus Group.

- **Safe attachments –** This policy protects the organisation from Potentially harmful attachments. Potentially harmful attachments will result in a replacement which will remove the attachment from the email before delivering it to the end-user advising that the attachment was removed. Attachments removed in this way can be later released by an admin/ Focus Group.

- **Safe links –** This policy protects our users from opening potentially unsafe links.
  This policy will scan all links in emails and rewrite them as a safe link for the user to click on. Users will be notified that their link has been re-written.

- **Antispam –** This policy will block messages based on a number of factors including the sending domain's mail reputation as well as the email's contents, etc.
  This policy will take action on any email with a spam score of 7 or higher. All potential spam items will be sent to the user's junk folder, prepending the subject line with additional text such as "[POTENTIAL SPAM]",

- If you think you may have compromised the safety of the home's bank details and/or have lost money due to fraudulent misuse of the debit card, you should immediately contact Head Office so that Jane can report it to the bank and cancel the card.

  NB Please note – all debit cards are in Jane's name, any dealings with the bank or police need to be carried out by Jane.

Sourced from actionfraud.police.uk

INTERNET SAFETY

It is important to be wary of malicious, criminal or inappropriate websites, especially when using devices belonging to Anderida:

- Check for presence of an address, phone number and/or email contact – often indications that the website is genuine. If in doubt, send an email or call to establish authenticity.
- Check that the website's address seems to be genuine by looking for subtle misspellings, extra words, characters or numbers or a completely different name from that you would expect the business to have.
- Roll your mouse pointer over a link to reveal its true destination, displayed in the bottom left corner of your browser. Beware if this is different from what is displayed in the text of the link from either another website or an email.
- If there is NO padlock in the browser window or 'https://' (which signifies that it is a secure link), do not enter personal or company information on the site.
- Websites that are likely to be malicious will request more personal information than usual such as username, password or other security details IN FULL. Avoid 'pharming' by checking the address in your web browser once the website is loaded. This will avoid ending up at a fake

site even though you entered the address for the authentic one – for example ‘eeBay’ instead of ‘eBay.

- If you are suspicious of a website, carry out a web search to see if you can find out whether or not it is fraudulent.
- Do not use websites that are advertised in unsolicited emails from strangers.
- You must not click on links to unknown websites, download large files or access inappropriate content using company equipment or networks.

Sourced from- getsafeonline.org

ADDITIONAL MEASURES

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to Head Office.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
- Avoid accessing suspicious websites.

IF YOU THINK YOU MAY HAVE COMPROMISED THE SECURITY OF THE ORGANISATION OR NOTICE ANY SUSPICIOUS ACTIVITY ON THE COMPUTER – YOU MUST IMMEDIATELY PULL THE INTERNET CABLE AND THE MAINS TO THE DEVICE. IT IS NOT ENOUGH TO SHUT DOWN IN THE NORMAL MANNER.

YOU MUST REPORT ANY SECURITY BREACH, SUSPICIOUS ACTIVITY OR MISTAKE YOU MAKE THAT MAY CAUSE A CYBER SECURITY BREACH TO JANE BETTLEY AT THE FIRST INSTANCE.

Security Awareness Training and Testing

The end user is the cause of 90% of Security Incidents. Therefore, we aim to increase the vigilance of our staff throughout the company by providing Cyber Security Awareness Training and Testing programme provided by Focus Group.

This training will be conducted in three stages:

Stage 1 – The Baseline Test.

The agenda of this stage is to raise awareness of the lack of knowledge around Cyber Threats within the company.

Stage 2 - Training.

All employees will receive an email with access to the online training which must be completed every 12 months for compliance reasons. The training not only covers email threats but everything that is relevant in modern day Cyber Security. Employees will also have to complete a 10-question quiz to pass the training.

Stage 3 – The Testing Stage.

The most important stage, as FOCUS GROUP engineers will send out bespoke emails to all employees once a month randomly. This stage is to ensure that all employees are staying vigilant. If staff fail the monthly test they are enrolled in further training.

Sourced from: Focus Group

Article 4 (12) of the General Data Protection Regulation defines a data breach as:

"A breach of security leading to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed".

WHAT A DATA BREACH IS

A data security breach can come in many forms, but the most common are as follows

- Loss of theft of hardcopy documents and/or other confidential material
- Data and/or sensitive documents, posted, emailed or faxed to the incorrect recipient
- Loss or theft of equipment on which data is stored
- Inappropriate sharing or dissemination, this also includes staff accessing information to which they are not entitled.
- Hacking, malware, data corruption
- Information is obtained by deception or "blagging"
- Equipment failure, fire or flood

Anderida Adolescent care is legally obliged under the GDPR to act in respect of such data breaches. This procedure sets out how we will manage a report of a suspected data security breach.

Circumstances may arise where an individual is unsure whether a certain situation and/or incident constitutes a breach of security, it is best practice to report it to the Data Protection Officer (Jane Bettley) or On Call if Jane is uncontactable. If there are any IT issues such as the security of the network being compromised focus should be informed immediately. (Email focusit@focus-grp.co.uk Telephone 0330 024 2004

RESPONSIBILITIES

Information users: All information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action needs to be taken to prevent further damage.

Home managers: Are responsible for ensuring that staff in their team act in compliance with this policy and assist with investigations as required.

Lead responsible officer: Will be responsible for overseeing management of the breach in accordance with the data breach management plan, suitable further delegation may be appropriate in some circumstances.

REPORTING A BREACH

It is important to report a breach in a time sensitive manner; this is to ensure a minimal amount of damage to the organisation. As a general rule, if the threat is not targeted at an individual or organisation it is unlikely that there is a risk of a data breach. Being aware of your actions as an individual is also critical in protecting the sensitive data of the organisation.

INTERNAL

- Suspected data security breaches should be reported promptly to the DPO (Jane Bettley) as the primary point of contact on 01323 410655 or info@anderidacare.co.uk. If the DPO is uncontactable, On Call should be contacted.
- The report (provided at the end of this document) must contain full and accurate details of the incident including who is reporting the incident and what classification of data is involved.
- Once a data breach has been reported an initial assessment will be made to establish the severity of the breach. All data security breaches will be centrally logged by the DPO, to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes.
- The data breach must be reported to the Information Commissioners Office, details on how to report this can be found via this link- https://ico.org.uk/

EXTERNAL

- If a severe data security breach is suspected, this must be reported to the Action fraud team via their website https://www.actionfraud.police.uk/ or by calling the National Fraud & Cyber Crime reporting centre on 03001232040.
- Notifications must be made 'without undue delay' and within 72 hours of becoming aware of it.
- If Anderida fail to do this then they must explain the reason for the delay.
- The data breach must be reported to the Information Commissioners Office, details on how to report this can be found via this link- https://ico.org.uk/

CONSEQUENCES

The company considers the following actions to be a misuse of its IT systems or resources:

- Any malicious or illegal action carried out against the company or using company systems
- Accessing inappropriate adult and illegal content within company premises or using company equipment
- Excessive personal use of company IT systems during core working hours
- Removing data or equipment from company premises or systems without permission, or in circumstances prohibited by this policy
- Using company equipment in a way prohibited by this policy
- Circumventing technical cyber security measures implemented by the company's IT team
- Failing to report a mistake or cyber security breach within the required time frame

ANY ANDERIDA EMPLOYEES FOUND TO HAVE ACTED IN BREACH OF THIS POLICY MAY BE SUBJECT TO DISCIPLINARY PROCEDURES OR OTHER SANCTIONS.

RESOURCES

Some parts of this policy were written with guidance from SEQ Legal https://seqlegal.com/

https://www.getsafeonline.org/

https://www.actionfraud.police.uk/

https://gdpr-info.eu/

https://ico.org.uk/media/fororganisations/documents/1562/guidance_on_data_security_breach_management.pdf

THIS POLICY IS DUE TO BE REVIEWED IN January 2023

DATA BREACH INCIDENT REPORT

STEPS:	NAME: ROLE:	DATE OF BREACH: DATE REPORT STARTED:
1)	**Summary of event and circumstances:** *Description of what happened, when, who?*	
2)	**Type of personal data:** *Describe the type of information and include the volume of information that has been breached - name, contact details and anything else that may be deemed as relevant.*	
3)	**Action taken by staff member:** *Was the matter reported in a time sensitive way and how?*	
4)	**Do Anderida have a policy/procedure in place to minimise risk:**	*YES / NO* *(please highlight)*
5)	**Has there been a breach of policy/procedure by officer/staff member?**	*YES / NO* *If yes, what action been taken?*
6)	**Have details of notification been given to the DPO (Jane Bettley)?**	*YES / NO* *If no, please explain why. What alternative route has been followed?*
7)	**Changes required following this incident to prevent further data breach:** *Summary of actions taken, and details of actions taken to enforce these changes.*	
8)	**Outcome following this incident:** *Date of report conclusion and details of outcome.*	