GROVE Neurodivergent Mentoring & Education LTD

ONLINE SAFETY

SCOPE & AIMS OF THIS POLICY:

GROVE takes a robust approach to our user's and staff's online safety. This policy is used in conjunction with GROVE's Privacy Policy, Data Projection Policy & other internal policies & procedures.

Importantly, all sessions where a single member of staff is in attendance are recorded for quality assurance, monitoring and safeguarding purposes. The recordings are only available to the CEO/DSL & where appropriate the staff member leading the session and will not be shared with users.

We ensure our staff are educated about four areas of risk and although we are not responsible for *educating* our users, where the need or opportunity arises, we will raise awareness and follow this up with contact home. Where a safeguarding concern arises we will follow our CP and Safeguarding Policy and Procedures. The four areas of risk are:

- **content:** being exposed to illegal, inappropriate or harmful content.
- **contact:** being subjected to harmful online interaction with other users.
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
- **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams (to be reported to the DSL/CEO and also reported to the Anti-Phishing Working Group https://apwg.org/).

Additional information: Safe remote learning hub - UK Safer Internet Centre

PRACTICAL CONSIDERATIONS & GENERAL ONLINE CODE OF CONDUCT

Staff must:

- Be able to rely upon a working computer and internet service with webcam, audio and headphones (headphones are only a requirement when others in your environment may overhear sessions) that is kept regularly up to date, with anti-virus software approved by GROVE;
- Ensure that firewalls are installed and the latest anti-malware protection is securing your devices.
- Not access, copy, remove or otherwise alter any other GROVE files without express permission;
- Only communicate with children/young people and parents/carers using official GROVE systems and not use personal email addresses, mobile phones (unless the number is withheld) or social media/networking sites for such communications;
- Not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, and contact the CEO if there are any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes);
- Not try to email, upload, download or use any content that:
  - is unlawful (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act);
  - is inappropriate;
  - that may cause harm or distress to others (this includes but is not limited to – violent, defamatory, vulgar, obscene, libellous, hateful, racist, threatening, vulgar, obscene, pornographic, invasive of another's privacy);
  - infringes any copyright laws (including music/videos), intellectual property, contractual relationships or other proprietary rights of any party;
  - contains software viruses or any other code, files or programmes designed to damage, interrupt, destroy or limit the functionality of any computer software/hardware or other such equipment;
  - poses or creates a privacy or security risk to any person or organisation;
  - would be considered 'spam';
  - or in the sole judgment of GROVE's CEO, is something that would negatively impact our user's safety or happiness whilst using our service or positions GROVE at risk of harm or liability in any way.
- Not engage in any on-line activity that may compromise professional responsibilities;

- Report any illegal, inappropriate or harmful material or incident you become aware of to the CEO/DSL;
- Any instances where a member of staff feel their actions, or the actions of others, may have compromised the organisation, or their own professional standing, details should be recorded and reported to the CEO/DSL.

PASSWORD / LOGIN SECURITY

- Password protect their device and Microsoft account: Passwords should be long. Good practice highlights that passwords over 12 characters in length are considerably more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack.
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised.
- Passwords must not include names or any other personal information about the user that might be known by others.
- Passwords must be changed on first login to the system.
- Do not disclose usernames or passwords to anyone else, nor use any other person's username and password.
- Do not write down or store a password where it is possible that someone may steal it. It may be good practice to use a 'password vault' to store encrypted passwords and generate very difficult to crack passwords.
- If you leave your computer you should lock the screen to ensure no accidental or unauthorised access.
- You should not share your computer with other people: they may innocently click on malicious links that may install malware onto your device. This would mean that a hacker would potentially have access to your work data. In any event, ensure that you have up-to-date anti-virus protection on your devices.
- If staff are concerned their login details may have been compromised, they must immediately change their password and report the situation to the CEO and DPO.

Additional information: Password Management & Security Guide | SWGfL

THE FOLLOWING GUIDANCE REFERS ONLY TO ONLINE SAFETY / ONLINE CODE OF CONDUCT, PLEASE REFER TO THE STAFF HANDBOOK AND OUR ADDITIONAL POLICIES FOR FULL GUIDANCE ON RUNNING SESSIONS.

BEFORE EVERY SESSION

- Sessions should be well prepared for, adhering to all guidance as outlined in the Staff Handbook, Staff Code of Conduct and the requirements noted in this policy. This includes but is not limited to:
  - Where pre-planned internet sites are in use staff must check these ahead of the session and thus users should be guided to sites checked as suitable for their use. Where a site is accessed without prior planning then reasonable care should be taken by not sharing the screen until the staff member is satisfied it is safe. There are processes in place for dealing with any unsuitable material that is found in internet searches in the Staff Handbook;
  - Ensuring that any content is age and developmental stage appropriate.
- Follow the protocol for sharing the session link as outlined in the Staff Handbook. The same link is used for all sessions with that user (unless there is a date breach) and this link must also be shared with the CEO/DSL;
- As per the Staff Handbook, ensure the session is set so that only the Mentor can record and share their screen and there is a waiting room/lobby before admittance (usernames that do not match the attendance register must not be admitted, users are asked to use their first name and can choose to add their pronouns);
- Complete connectivity and technology checks in good time before commencing sessions and follow the Session Guide if there are problems;
- Ensure your environments does not display any inappropriate images, documentation or other item – ideally a blurred or appropriate picture should be used as a background;
- Ensure you have appropriate clothing on top and bottom that could not be considered obscene, offensive, suggestive or provocative. We encourage the use of comfortable clothing that does not have logos/pictures or writing;

- Ensure personal items that could identify you or your location are not visible in the background;
- Ensure personal distractions and disturbances are minimised;
- Use a headset or headphones when other people are present in your environment – it would be considered a data breach for other people to be able to hear your Mentee(s);
- Only ever use the authorised delivery platform;
- Set your display name as your first name only with your pronouns if you want to share these (do not use your surname).

DURING EVERY SESSION

- As per the Staff Handbook, remind all users at the start of the session:
    - It is being recorded;
    - They must abide by the User Code of Conduct;
    - They are not permitted to screen shot, record, photograph any content (if it is suspected to be the case the staff member must immediately remove the child/young person, record this as outlined in the Staff Handbook and contact parents/carers/guardians).
- Confirm the identity of all users once admitted from the waiting room (remember not to admit anyone who has a different username to that on the attendance register – it should show their first name and optional pronouns only)– those who choose to have a camera off will need to be confirmed via a quick visual check of the young person or by a visual check of the parent/carer/guardian;
- If you cannot confirm identity, then follow the Staff Handbook guidelines for contacting parents/carers/guardians;
- Once the session begins, check all users:
    - Are fully dressed and wear suitable clothing, as should anyone else visible in the background;
    - Confirm where possible that they are in appropriate areas, for example not in bedrooms with closed doors and if you are at all concerned about their location follow the Staff Handbook guidance;
    - Are not displaying any inappropriate images, documentation or other item – ideally their background should be blurred/an appropriate picture;
    - Are not showing personal items that could identify an individual are not visible in the background;
    - Remove any duplicate logins (users are not permitted to access the session from a separate device);
    - Follow the guidelines in the Staff Handbook if there are any concerns in these areas.
- Adhere to the pre-agreed policy for the recording of sessions as outlined in GROVE's Staff Handbook and report any error with recording immediate to the CEO/DSL. Repeated failure to record sessions may result in disciplinary action;
- Follow the procedures outlined in the Staff Handbook and Child Protection and Safeguarding Policy if you become concerned about anything you see or hear.

AFTER EVERY SESSION

- Make notes on any issues with recording, registration, behaviour and safeguarding immediately following the session;
- Notes must only be made on official GROVE platforms. Handwritten notes must immediately be transferred and destroyed (see our Data Protection Policy).

QUALITY ASSURANCE & MONITORING:

All session links are shared with the CEO/DSL via access to your Microsoft account.

The CEO/DSL can join a session at any point without notifying the member of staff. The DSL/CEO may join without interruption or if it feels more appropriate greet the children/young people and observe a portion of the session. The CEO/DSL will be mindful of the impact this may create for the children/young people and will therefore communicate this to parents/carers/guardians ahead of the session in order that the children/young people have prior notice.

The CEO/DSL also regularly reviews recorded sessions. The reason for this is to assure quality of service and safeguarding as per the Staff Handbook.

Staff experience will also be considered when plans for quality assurance and monitoring are made but never to the detriment of our user’s welfare.