ONLINE SAFETY POLICY

SCOPE & PURPOSE

1. Sheldrake Training recognises the benefits and opportunities that new technologies offer to teaching and learning. We encourage the use of technology in order to enhance skills and promote achievement. However, the accessible and global nature of the internet and the variety of technologies available, mean that we are also aware of potential risks and challenges associated with such use.

2. The purpose of this policy is to:

   a. Ensure the safety and wellbeing of young people is paramount when adults, young people or children are using the internet, social-media or mobile devices.

   b. Provide staff and volunteers with the overarching principles that guide our approach to online safety.

   c. Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

3. Our approach is to implement safeguards within Sheldrake Training and to support staff and learners to identify and manage risks independently. We believe this can be achieved through a combination of security measures, training and guidance and the implementation of our associated policies. In furtherance of our duty to safeguard learners and protect them from the risk posed by extremism and radicalisation, we will do all that we can to make our learners and staff stay safe online and to satisfy our wider duty of care.

4. This online safety policy should be read in conjunction with other IT policies as well as the Safeguarding and Prevent Policies, IT Acceptable Use Policy, Staff Disciplinary and Dismissal Procedures.

5. This policy covers:

   a. Anyone logging into any network, service, website, or portal associated with Sheldrake Training.

   b. Connecting a device via Sheldrake Training network.

   c. Any electronic communication with a Sheldrake Training Learner, member of Staff or contractor.

   d. From any RACPD or Sheldrake Training geographic location.

6. This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in the UK including but not extant to: Communications Act 2003, Malicious Communications Act 1989, KCSIE 2023, Childcare Act 2004, Criminal Justice Act 1988.

RESPONSIBILITIES

7. The reporting responsibilities for online/e-safety follow the same lines of responsibility as Sheldrake Training Safeguarding and Prevent policy.

8. All staff are responsible for ensuring safety of learners and must:

a. Report any concerns or disclosures immediately to the Designated Safeguarding Lead (DSL) or Designated Safeguarding Officer (DSO) – the report format contained in Sheldrake Training Safeguarding Policy and Procedures should be used.

b. Never offer assurance of confidentiality, everything discussed must be reported.

c. Keep to the terms and conditions of the IT Acceptable Use Policy at all times.

d. Attend staff training on e-safety and display a model example to learners at all times.

e. Actively promote through embedded good e-safety practice into inductions and throughout training.

f. Ensure learners always act safely and responsibly when using the internet and/or mobile technologies.

g. Communicate with learners professionally and in line with Sheldrake Training Communications Policy at all times.

9. All learners must:

a. Keep to the terms and conditions of the IT Acceptable Use Policy at all times.

b. Receive appropriate online guidance as part of their programme of study.

c. Inform a member of staff where they are worried or concerned an e-safety incident has taken place involving them or another member of the community.

d. Act safely and responsibly at all times when using the internet and/or mobile technologies.

10. The IT Manager is responsible for:

a. Ensuring Sheldrake Training IT infrastructure is secure and meets appropriate industry standards.

b. IT security incidents are recorded, investigated, and resolved within reasonable a reasonable timescale.

11. The DSL or DSO are the persons responsible for monitoring any investigation of online safety incidents and will follow the reporting procedure laid down in the Safeguarding Policy (see Annex A for flowchart). The DSL/DSO have a duty to escalate incidents external following government guidelines should they feel it appropriate.

MONITORING

12. Sheldrake Training activity monitor, log and report on learners and staff use of IT systems and IT network usage as part of the responsibility towards the ‘safeguarding of young people and vulnerable adults’ and Prevent duty for terrorist and extremist behaviour.

13. An attempt to interfere or avoid the monitoring or logging of any IT systems will be referred to Sheldrake Training disciplinary process.

14. Where requested this information will be securely shared with appropriate local authorities and external support agencies.

REPORTING

15. If online abuse occurs, we will respond to it by:

a. Having clear and robust safeguarding procedures in place for responding to abuse (including online abuse).

b. Providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse, and sexual exploitation.

c. Making sure our response takes the needs of the person experiencing abuse and any by standers and our organisation as a whole into account.

d. Reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

CYBER SECURITY

16. Sheldrake Training IT systems are certified to meet the Information Security and Cyber Security standards - Cyber Essentials Scheme.

17. These standards are reviewed annually by independent experts providing staff, learners and trustees with reassurance that Sheldrake Training IT systems cyber security follow the highest levels of best practice.

18. Any breach of the Computer Misuse Act 1990 including all forms of hacking or acquiring / accessing someone else's digital identity is a criminal offence and will be referred to Sheldrake Training disciplinary procedure and sent to the police for investigation.

TRAINING

19. Learners will be provided with online 'e-safety' guidance by staff at induction and via an online learning padlet. Planning will include appropriate and relevant online guidance for learners throughout their programme of learning.

20. Issues associated with E-safety apply across the curriculum and learners should receive guidance on what precautions and safeguards are appropriate when making use of the internet and mobile technologies. Learners should also know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search.

21. Within classes, learners will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

STAFF

22. Staff will receive an introductory session for digital learning/working systems and environments within the induction period. This introductory session will signpost the Online Safety Policy and provide an overview for all staff. Each member of staff must record the date of the training attended on their CPD log.

23. Any new or temporary users will also be asked to review and undertake basic online training and sign to confirm that they have read and understand both the online safety policy and the IT acceptable Use policy.

BEHAVIOUR

24. Use of any RACPD or Sheldrake Training IT equipment and systems is conditional to the policies including the IT Acceptable Use Policy, IT Security Policy, Prevent and the Discipline Policy.

25. Communications by staff and learners should be always courteous and respectful whether offline or online. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the Discipline Policy.

CYBER BULLYING

26. Cyber bullying is a form of bullying. As it takes place online, it is not confined to RACPD teaching or working hours. Cyber bullies can communicate their messages to a wide audience with speed and often remain anonymous or unidentifiable. Cyber bullying includes bullying via:

a. Text message and messaging apps e.g. sending unwelcome texts or messages that are threatening or cause discomfort.

b. Picture/video-clips e.g. using mobile device cameras to bully someone, with images usually sent to other people or websites.

c. Phone calls, e.g. silent calls, or abusive messages. The bully often disguises their number.

d. Email e.g. emailing upsetting messages, often using a different name for anonymity, or using someone else's name to pin the blame on them.

e. Chat room e.g. sending upsetting responses to people when they are in a web- based chatroom.

f. Instant Messaging (IM) e.g. sending unpleasant messages in real-time conversations on the internet.

g. Websites e.g. insulting blogs, personal websites, social networking sites and online personal polling sites.

27. Where conduct is found to be unacceptable, Sheldrake Training will deal with the matter internally and refer to relevant policies, for example, the Disciplinary and Dismissal Policy. Where conduct is considered illegal, RACPD will report the matter to the police.

SAFEGUARDING & PREVENT

28. Staff should beware of Sheldrake Training's responsibility of the Prevent Duty and Safeguarding of young people and adults at risk. The following guidance must be adhered by all staff communicating online. Staff should:

a. Not post any personal views, beliefs, or opinions.

b. Challenge any personal views, beliefs or opinions posted by learners.

c. Refer any post considered to isolate or put a young person or vulnerable adult at risk to a DSL/DSO for further investigation.

d. Refer any post considered to promote extreme views to the DSL/DSO for further investigation.

ONLINE COMMUNICATION

29. Online communication must:

a. Be concise.

b. Be engaged and use appropriate language.

c. Use decent-quality images whenever possible.

d. Use English, correct spelling and grammar.

e. Follow the appropriate style and brand guidelines.

GDPR

30. Before contacting any individual, you must have a “Lawful basis for processing” the contact information. For more information refer to https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

31. **Do’s and Don’ts**. The points below offer guidance on appropriate use of online communication. Any breach of this guidance will be referred to Sheldrake Training disciplinary procedure. Any breach considered to be a criminal offence will be referred to the police for investigation. The appropriate use of communication applies to all devices and services, which might include; computers, laptops, mobile devices (including phones and tablets), game consoles, email, instant/direct messages, chat rooms & social media. Examples are:

a. You must not create, store, exchange, display, print or circulate any message or media which may cause offense to others.

b. You must not post or circulate any message which may be considered harassment.

c. You must not send messages at random or excessively, also referred to as "spamming".

d. Staff must not use personal devices or accounts as a method of communicating with students.

e. Staff and students must not make or receive personal calls, messages, or emails etc. whilst in a teaching environment.

f. RACPD or Sheldrake Training devices may, on occasion, be used to gather either video or photographic evidence in order to support students’ course requirements provided that RACPD hold a signed authorisation form for the student in question. All personal images will be held in accordance with Sheldrake Training Privacy Statement.

g. You must not give out any personal information such as contact details, financial information, or passwords (however this is not an extensive list).

h. You should not open files or emails from people you do not know. They may contain viruses or offensive material.

i. If you see something abusive or upsetting online, you must report it.

j. You should not save your log-on details on shared computers as some people may use your screen name to defraud or scam people in your contact lists.

k. There may be legal implications if the Internet is used for criminal intensions for example to intimidate or to extract financial information for personal gain. All conversations using RACPD or Sheldrake Training IT systems are captured and recorded on the servers.

l. You must own the copyright of any material you post.

m. You must not post any confidential information to any online platform.

32. If your post could be considered as representing or being associated to RACPD in any way, then:

a. It is imperative to portray a balanced tone when raising politically sensitive issues.

b. When linking to websites not controlled by the RACPD or Sheldrake Training Group (such as to relevant news articles) it must be clear that the link is external.

c. No communication should be made with learners from personally created user accounts.

33. Only approved online messaging services can be used to communicate with students, all communication must be via an RACPD or Sheldrake Training user account these include Texting services, Zoom, Microsoft Teams and Microsoft Office 365 collaboration.

SOCIAL MEDIA

34. Only employees who have been authorised to use social media accounts through the RACPD social media approval process may access social media on the RACPD or Sheldrake Training network or create, maintain, or post on behalf of official RACPD or Sheldrake Training accounts.

35. The use of social media will only be approved where it is deemed to benefit learners and learning, is in the business interests of Sheldrake Training, and meets safeguarding and PREVENT duties. There are a number of official social media communications channels, which are part of RACPD infrastructure. These take priority in externally published documents and materials.

36. In the event of an incident or emergency involving RACPD or Sheldrake Training Group no content should be posted to any social media channels except by the Marketing and Communications team who will manage PR centrally

ONLINE PRIVACY AND PERSONAL INFORMATION

37. Sheldrake Training employees and learners are expected to respect Sheldrake Training reputation when posting online. Any information which may be consider damaging Sheldrake Training reputation may result in disciplinary and/or legal action. Use of Sheldrake Training Intellectual Property (IP) must be requested and approved by Marketing. Any use of IP without permission may result in disciplinary and/or legal action.

38. Employees of Sheldrake Training must maintain professional boundaries at all times, particularly when accepting or inviting 'friend' connections on personal social media accounts.

39. Employees must not passively or actively connect on social media with current or ex- students who are under the age of 18 or who have a vulnerability, adult students who they teach, support or could be deemed to give unfair advantage to, or any other persons deemed inappropriate by the DSL or DSO.

40. Acts of a criminal nature or any safeguarding concerns may be referred to the police, Local Safeguarding Adult and Children Board (MASH) and/or the Independent Safeguarding Authority.

41. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe – e.g. there are particular risks where personal images are posted onto social networking sites.

42. No image/photograph can be copied, downloaded, shared or distributed online without permission from the owner of that image. Photographs of activities on RACPD or Sheldrake Training premises should be considered carefully and have the consent of both the Management Team/Marketing Department and learner before being published. Approved photographs should not include names of individuals.

43. Personal information will be held and processed in accordance with the General Data Protection Regulation (GDPR) 2018. For more information please refer to the Sheldrake Training Privacy Statement available on the website www.racpd.org.uk

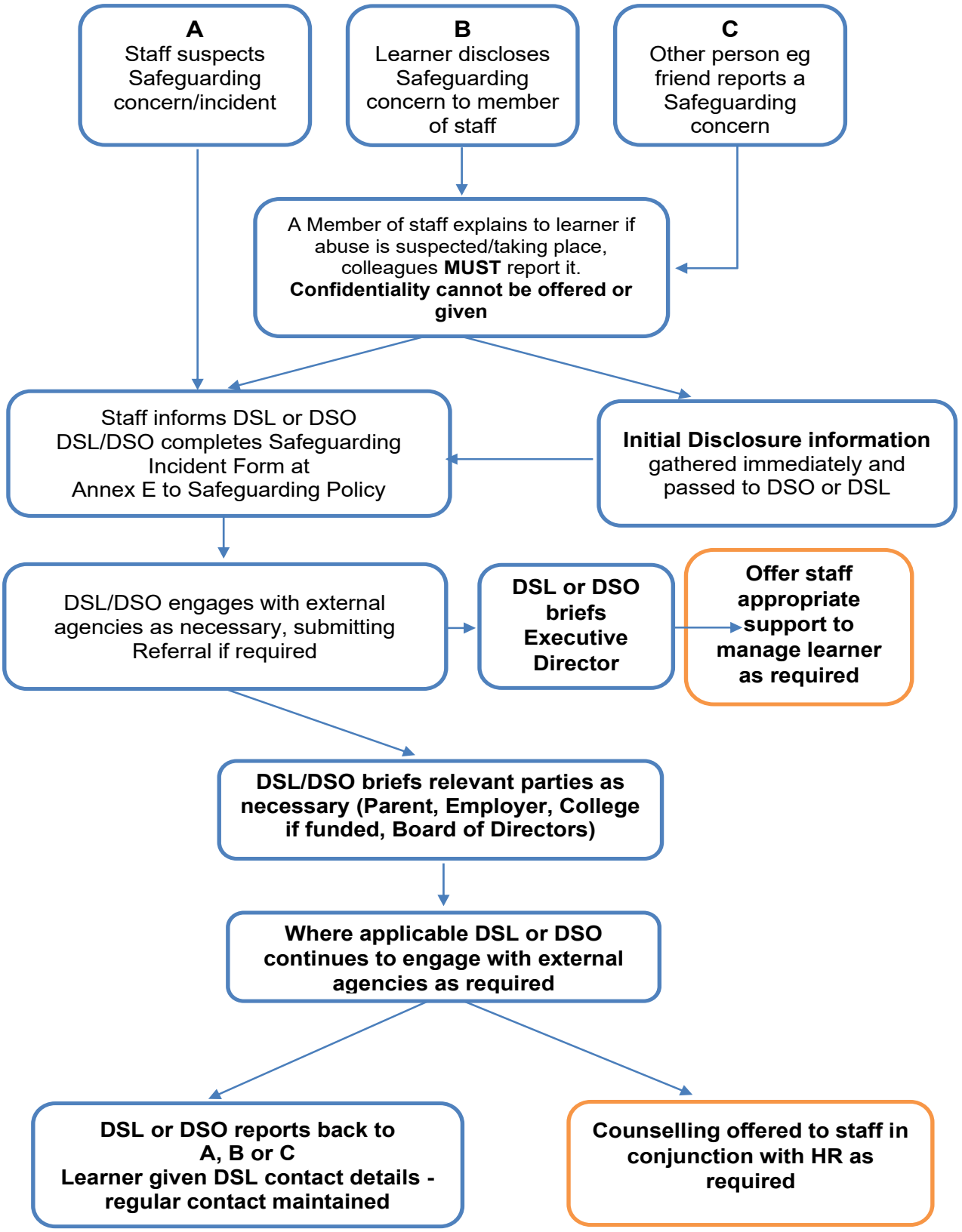
FEEDBACK AND FURTHER INFORMATION

Sheldrake Training welcomes all constructive feedback on this and any other policy. If you would like further information on IT Safety, or wish to send us your comments, then please contact the facilities manager on 01980 845789.

Version Control	
Policy Title:	Online Safety Policy
Version Number:	Ver 3.1
Originator:	HR Manager
Approved by:	Training Director
Date Approved:	9 May 2025
Review Interval:	Annually or when regulatory changes
Review Date:	May 2026

Annex:

A. Safeguarding Procedures for Learners (Updated Nov 25).

ANNEX A
TO ONLINE SAFETY POLICY

SAFEGUARDING PROCEDURE FOR LEARNERS – FLOWCHART (Annex C to Safeguarding Policy)