Go Fish Education Ltd

Acceptable Use Policy

Teaching and Support Staff
Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current online safety policy and practices
- they report any suspected misuse or problem to Kerry Brown or Dylan Brown for investigation/action/sanction
- all digital communications with pupils/parents/carers should be on a professional level and only carried out using official systems

Education – Students/Pupils

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided within key curriculum areas and include:

- Key online safety messages which will be reinforced during learning sessions
- Students will be taught to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students will be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

Education & Training – Staff
It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy.

Mobile Technologies

- Mobile phones may be used for research and educational purpose

Use of digital and video images

- When using digital images, staff will inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the website/social media/local press

Data Protection

Further information can be found in the Go Fish Education GDPR Privacy Policy.

When personal data is stored on any mobile device or removable media the:

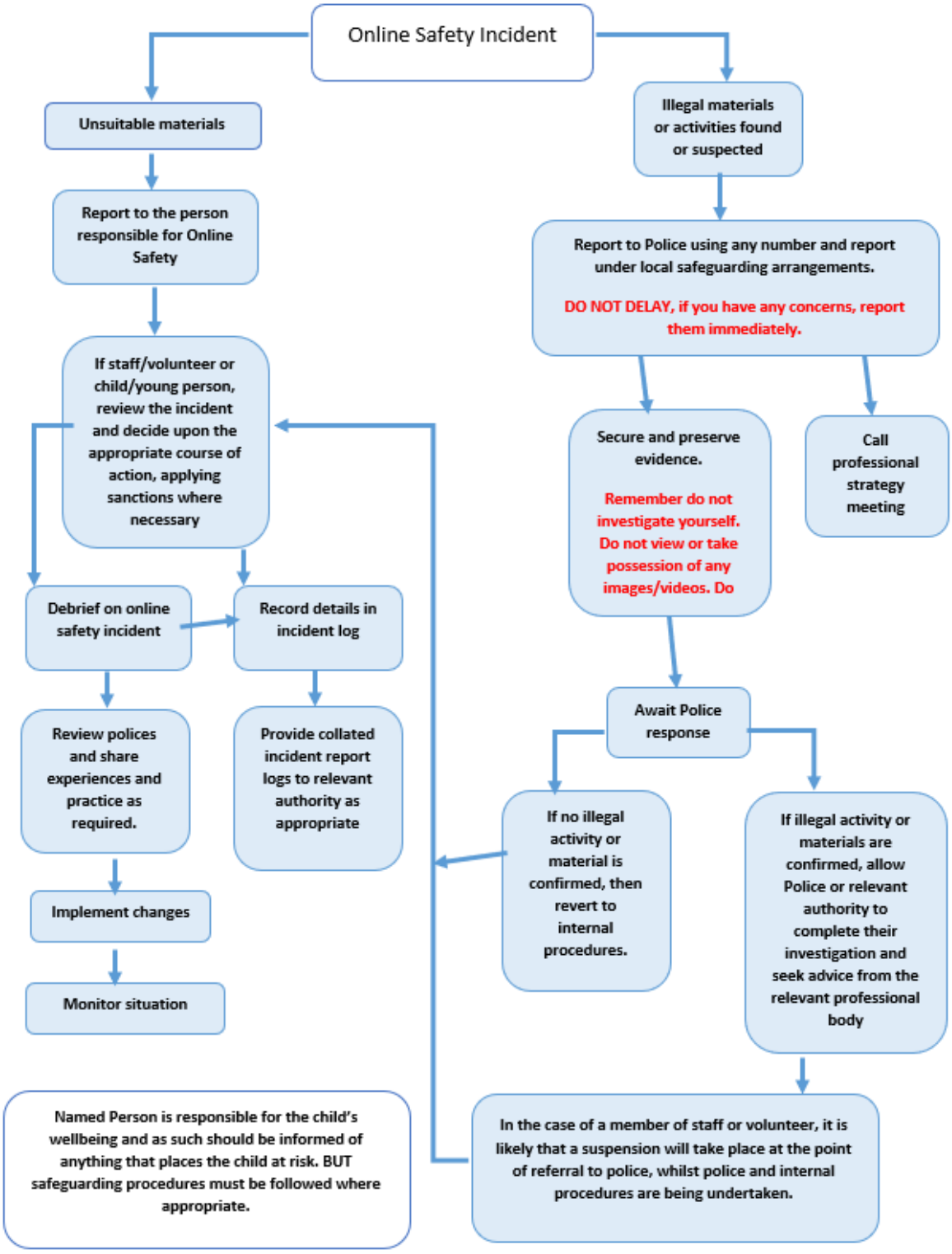
- data must be encrypted and password protected.
- device must be password protected.
- device must be protected by up to date virus and malware checking software
- data must be securely deleted from the device, in line with policy (below) once it has been transferred or its use is complete.

Staff must ensure that :

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to
- can help data subjects understands their rights and know how to handle a request whether verbal or written.
- where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- will not transfer any Go Fish Education personal data to personal devices except as in line with policy
- access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Policy dated: March 2023
Review date: July 2023