SHREE SWAMINARAYAN VIDYALAY

E-SAFETY POLICY

Version control

Date of introduction of this policy	November 2021
Revised	October 2024
Date for next review of this policy	October 2025
Policy owner	Designated Safeguarding Lead
Policy owner (Proprietors)	Board of Directors

Policy Statement

The internet, mobile phones, social networking and other interactive tools and spaces have transformed the way in which we live.

Children and young people are among the early adopters of the new technologies and move effortlessly between the various interactive services and devices to communicate, create, and share content with family and friends.

Whilst most children and young people use the internet responsibly and safely, it is essential that all potential risks are recognised, identified, and mitigated and that staff and volunteers feel confident about evaluating e-safety and seeking help when needed.

1. Purpose of Policy

The online safety policy should be recognised as a safeguarding policy, not a technical or computing policy and falls within the role and responsibilities the Designated Safeguarding Lead (DSL). The purpose of Shree Swaminarayan Vidyalay ("SSV") online safety policy is to:

- Ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Ensure that SSV operates in lines with its values and within the law in terms of how we use online devices.
- Identify clear procedures to use when responding to online safety concerns.

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on:

- Online abuse
- Bullying
- Child protection

SSV identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate, or harmful material
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

2. Policy Scope

- SSV believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- SSV identifies that the internet and associated devices, such as computers, tablets, mobile phones, and games consoles, are an important part of everyday life.

- SSV believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.

3. Monitoring and Review

- SSV will review this policy at least annually.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- The named trustee for safeguarding will report on a regular basis to the trustee body on online safety practice and incidents, including outcomes.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) / Nominated Safeguarding Lead Person (NSP) (Vikesh Wagjiani) has lead responsibility for online safety.
- Shree Swaminarayan Vidyalay recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

Password policy

From year 2021, all learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.

We encourage all users to:

- Use strong passwords for access into our system.
- Change their passwords every 90 days.
- Always keep their password private; users must not share it with others or leave it where others can find it.
- Not to login as another user at any time.

Publishing Images and Videos Online

We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: codes of conduct/behaviour.

Managing Email

Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including code of conduct/behaviour policy.

The forwarding of any chain messages/emails is not permitted.

- Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- Setting email addresses and other official contact details will not be used for setting up personal social media accounts.

- Members of the community will immediately tell Vikesh Wagjiani, DSL, if they receive offensive communication, and this will be recorded in our safeguarding files/records.

Educational use of Videoconferencing and/or Webcams

- SSV recognise that videoconferencing and/or use of webcams can be a challenging activity but brings a wide range of learning benefits.
- All videoconferencing and/or webcam equipment will be switched off when not in use and will not be set to auto-answer.
- Videoconferencing contact details will not be posted publicly.
- Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

Users

- Parents/carers consent will be obtained prior to learners taking part in videoconferencing activities.
- Learners will ask permission from a member of staff before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately, according to the learners age and ability. This will be achieved by:
    - Ensuring that the meeting rooms are open to members only.
    - Presentation is only done by teachers (unless deemed necessary)
    - Chat functionality will be limited to Meeting-in Only
- Only key administrators will be given access to videoconferencing administration areas or remote-control pages.

Content

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.

Management of Applications (apps) used to Record Children's Progress

- We use Microsoft Teams to track learners progress and share appropriate information with parents and carers.

To safeguard learner's data:

- Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

Learners Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources.
- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for learners under this age.
- Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
- Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Learners will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
    - To use safe passwords.
    - To use social media sites which are appropriate for their age and abilities.
    - How to block and report unwanted communications.
    - How to report concerns both within the setting and externally.

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

- Having clear and robust safeguarding procedures in place for responding to abuse
- 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.
- Making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account.
- 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.

Signed on behalf of the Management Committee:

Name: Vikesh Wagjiani Signature: V.R. wagjiani Date: 29 October 2024