SKYLARK FEDERATION

Online Safety Policy

Date of policy: September 2026

Date for review: September 2027

Statutory Framework: This policy is compliant with statutory DfE guidance *Keeping Children Safe in Education (KCSiE 2026)*, *Meeting Digital and Technology Standards in Schools*, the *Data (Use and Access) Act 2025*, the *Data Protection Act 2018*, and the *UK GDPR*.

1. Aims of the Policy

The purpose of this 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, artificial intelligence (AI), or mobile devices.
- Provide staff and volunteers with the overarching principles that guide our approach to online safety, filtering, monitoring, and digital literacy.
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices and emerging technologies.

The policy statement applies to all staff, volunteers, children, and young people, and anyone involved in the Skylark Federation's activities.

2. Legal Framework & Safeguarding Principles

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 NSPCC Learning regarding online abuse, bullying, and the child protection system.

We believe that:

- Children and young people should never experience abuse of any kind.
- Children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- The online world provides everyone with many opportunities; however, it can also present risks and challenges (including cyberbullying, grooming, radicalisation, online misogyny/misandry, and AI-enabled abuse).

- We have a duty to ensure that all children, young people, and adults involved in our organisation are protected from potential harm online.
- We have a responsibility to help keep children and young people safe online, whether or not they are using the Skylark Federation's network and devices.
- Working in partnership with children, young people, their parents, carers, and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.
- All children, regardless of age, disability, gender reassignment, race, religion or belief, sex, or sexual orientation, have the right to equal protection from all types of harm or abuse.

Contextual Safeguarding Considerations:

To ensure equal protection, staff receive guidance and resources tailored to specific pupil groups, including:

- Safeguarding children who come from Black, Asian, and minoritised ethnic communities.
- Safeguarding d/Deaf and disabled children and young people.
- Safeguarding LGBTQ+ children and young people.
- Safeguarding children with special educational needs and disabilities (SEND).

3. Operational Online Safety Commitments

We will seek to keep children and young people safe by:

- Appointing an **Online Safety Coordinator / Designated Safeguarding Lead (DSL)**, who will oversee the online safety strategy and coordinate the work of the school, making use of the NSPCC, our schemes of learning for PSHE, and other sources of information as appropriate.
- Providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults and Acceptable Use Policy.
- Supporting and encouraging the young people using our service to use the internet, social media, and mobile phones in a way that keeps them safe and shows respect for others.
- Supporting and encouraging parents and carers to do what they can to keep their children safe online.
- Developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child or young person.
- Reviewing and updating the security of our information systems regularly.
- Ensuring that usernames, logins, email accounts, and passwords are used effectively.
- Ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate.
- Ensuring that images of children, young people, and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given.
- Providing supervision, support, and training for staff and volunteers about online safety.
- Examining and risk assessing any social media platforms, software, and new technologies (including Generative AI tools) before they are used within the organisation.

4. Generative Artificial Intelligence (AI) and Emerging Technologies

- **Acceptable Use of AI:** Staff and pupils using AI systems for educational purposes must ensure compliance with data privacy regulations. No personal, sensitive, or identifiable pupil data may be inputted into public AI models.
- **AI-Enabled Harm & Deepfakes:** The creation, manipulation, or distribution of synthetic nudes, semi-nude images, or deepfakes using Generative AI is strictly prohibited. Any incident involving AI-generated image abuse or sexual harassment will be managed immediately as a severe safeguarding incident requiring a formal risk assessment under Child-on-Child Abuse protocols.

5. Filtering and Monitoring Standards

We use a filtering system to block access to inappropriate content, such as pornography, violence, hate speech, extreme views, and self-harm material. The filtering system is regularly reviewed and updated to ensure that it is effective. Harrap is our IT provider. We use Watchguard to filter our internet.

We also monitor pupil activity online. This is done to ensure that pupils are using the internet safely and responsibly. The school uses a variety of monitoring methods, including:

- **Network monitoring:** This involves monitoring the school's network traffic to identify any suspicious activity.

- **Device monitoring:** This involves using software to monitor the activity of devices that are connected to the school's network.
- **Physical monitoring:** This involves staff members monitoring pupils' screens when they are using the internet.

Our filtering and monitoring systems are designed to protect pupils from harm. However, it is important to note that no system is perfect. Pupils should still be aware of the risks associated with online activity and should report any concerns to a trusted adult immediately.

Governance and Annual Review: In accordance with KCSiE requirements, a named member of the Senior Leadership Team (SLT), alongside the DSL and Harrap IT, conducts a mandatory **Annual Filtering and Monitoring Review**. Written records of system tests, risk assessments, and blocklist audits are maintained and reported annually to the Governing Body.

6. Responding to Online Abuse & Cyberbullying

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

- Having clear and robust safeguarding procedures in place for responding to abuse (including online abuse).
- Logging all concerns immediately on CPOMS. Incidents involving sexting, youth-produced sexual imagery, or AI deepfakes will follow statutory triage guidance without viewing, copying, or forwarding imagery unnecessarily.
- 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.

7. Additional Filtering and Monitoring Guidance for Parents

Parents can also use filtering and monitoring software at home to help keep their children safe online. There are a number of different software packages available, so it is important to choose one that is right for your family.

When choosing filtering and monitoring software, it is important to consider the following factors:

- **The age of your children:** Different software packages are designed for different age groups.
- **The types of devices that your children use:** Make sure that the software you choose is compatible with the devices that your children use.
- **Your budget:** Filtering and monitoring software can range in price from free to expensive.

Once you have chosen a filtering and monitoring software package, it is important to set it up correctly. Be sure to read the instructions carefully and to contact the software provider if you have any questions.

By using filtering and monitoring software, you can help to protect your children from the risks associated with online activity. However, it is important to remember that no system is perfect. You should also talk to your children about online safety on a regular basis and monitor their online activity.

Tips for parents to help their children stay safe online:

- Talk to your children about online safety on a regular basis.
- Set clear rules for internet use at home, such as how long they can use the internet each day and what websites they can visit.
- Monitor your children's online activity by checking their browser history and social media accounts.
- Use parental controls to block inappropriate content and limit access to certain websites and apps.
- Teach your children how to be critical of the information they see online.
- Encourage your children to come to you with any concerns they have about their online safety.

8. Related Policies and Procedures

This policy statement should be read alongside our organisational policies and procedures, including:

- Child Protection and Safeguarding Policy
- Procedures for responding to concerns about a child or young person's wellbeing
- Dealing with allegations of abuse made against a child or young person

- Managing allegations against staff and volunteers
- Code of conduct for staff and volunteers
- Federation Behaviour & Anti-Bullying Policy
- Child-on-Child Abuse Policy
- Photography and image sharing guidance
- Data Protection & GDPR Policy