Version	Date	Updated by
1.0	13-09-23	Julia Whitesides

Online safety policy including social media

Links with other policies

- Relationship Education policy
- PSHE Policy
- Anti-Bullying Policy

Online Safety (e-Safety) policy statement

The aim 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 or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.
- Deliver an effective approach to internet safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

This policy:

- Applies to all staff/all online communications which directly/indirectly, represent Silver Linings School
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education.
- Defines the monitoring of public social media activity pertaining to Silver Linings School.

Definitions

- Silver Linings School defines "social media" as any online platform that offers real-time interaction between the user and other individuals or groups including but not limited to:
    - Online discussion forums.
    - Collaborative spaces, such as Facebook/Meta
    - Media sharing services, such as YouTube.
    - 'Micro-blogging' applications, such as X (formerly Twitter)

- Silver Linings School defines “cyber bullying” as any use of social media or communication technology to bully an individual or group.
- Silver Lining School defines “members of the school community” as any teacher, member of support or any other staff, pupil, parent/carer of pupil, governor or ex-pupil.

Legislation and Guidance

The Education and Inspections Act 2006 empowers the Headteacher to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other internet safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

How we keep children safe online

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and approach to online safety empowers the school and protects and educate students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate. KCSIE 2023 groups the threats into four C’s as follows:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes’.

- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

- **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

The school will ensure online safety is a running and interrelated theme whilst devising and implementing policies and procedures.

This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead and any parental engagement.

We will take the following actions to achieve these goals:

1. provide clear and specific directions to staff and volunteers on how to behave online through our staff code of conduct
2. have appropriate filters, safety systems and control over devices
3. an expectation of handing in any electronic devices and phones on arrival at school (see behaviour policy)
4. support and encourage 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
5. support and encourage parents and carers to do what they can to keep their children safe online
6. agree an online safety agreement for use with young people and their parents/carers- see appendix 2
7. develop clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person.

Roles and Responsibilities

Proprietor/Governance

The Proprietor are responsible for the approval of the Online safety Policy and for reviewing the effectiveness of the policy. A member of the Governance has the role of Online safety monitor. The role of the Online safety monitor will include:

- regular meetings with the DSL
- regular monitoring of online safety incident logs
- responsibility for ensuring that the Online Safety Policy, as written, does not discriminate on any grounds, including but not limited to: ethnicity/national origin, culture, religion, gender, disability or sexual orientation.
- Governance has responsibility for handling complaints regarding this policy.

The Headteacher

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and will be responsible for the day-to-day implementation and management of the Online Safety Policy and procedures of Silver Linings School.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see Appendix 1 flow chart on dealing with online safety incidents)
- The Headteacher is responsible for ensuring that staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- Take a lead role in investigating any reported incidents.
- Make an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.

Staff

- Must have an up-to-date awareness of internet and online safety matters and of the current school Online safety policy.
- Must have read, understood and signed the Staff Acceptable Usage Policy.
- Report any suspected misuse or problem to the Headteacher.
- Should only communicate online with pupils/parents/carers on a professional level and only carry this out using official school systems (school phone or school email).
- Have internet and online safety issues embedded in all aspects of the curriculum and other activities.
- Ensure that pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (upper KS2).
- Monitor the use of online technologies, mobile devices, cameras etc. in lessons and other school activities.
- Should plan ahead for lessons where internet use is required so that websites can be checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Should report and record online safety incidents using the school system.

Pupils

- Are responsible for using the school online technology systems appropriately and sensibly.
- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (upper KS2 children).
- Should know the importance of reporting any worries, abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices.
- They should also know and understand policies on the taking/use of images and on cyber-bullying.

- Should understand the importance of adopting good internet and online safety practice when using online technologies out of school.

Designated Safeguarding Lead

Designated Safeguarding Leads should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the importance of online/online safety. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- online and video images taken at school events
- access to parents' sections of the website

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International
- Keeping children safe online- Safer schools website and APP

Educating Pupils about Online Safety

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 in the following ways:

- A planned online safety curriculum should be provided as part of PSHE/other lessons and should be regularly revisited.
- Key online safety messages should be reinforced as part of a assemblies and pastoral activities.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be helped and encouraged to adopt safe and responsible use both within and outside school.

- Staff should act as good role models in their use of online technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. Classroom cloud or other filtering system will be used to block unsuitable sites and record children's searches.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the block is temporarily removed to those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

TOP TIPS for teaching Online safety

We encourage pupils to take a SMART approach to social media behaviour:

- **Safe** – Do not give out personal information, or post photos of yourself to people you talk to online. Follow age restriction rules.
- **Meeting** – Do not meet somebody you have only met online. We encourage parents/carers to speak regularly to their children about who they are talking to online.
- **Accepting** – We advise that pupils only open emails and other forms of communication from people they already know.
- **Reliable** – We teach pupils about the dangers of believing everything they see online.
- **Tell** – We encourage pupils to tell a teacher, parent or carer if they see anything online that makes them feel uncomfortable

Educating Parents about Online Safety

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring /regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website
- Parents'/Carers' sessions (if required)
- High profile events e.g. Safer Internet Day
- Reference to the relevant websites/publications e.g.
  www.swgfl.org.uk
  www.saferinternet.org.uk/

http://www.childnet.com/parents-and-carers

- The school website will provide online safety information for the wider community

Social Media Use – Staff

- Staff may not access social media during lesson time, unless it is part of a curriculum activity. Staff may use social media during their break times on their personal devices. Members of staff should avoid using social media in front of pupils.
- Members of staff must not "friend" or otherwise contact pupils or parents/carers through social media. If pupils or parents/carers attempt to "friend" or otherwise contact members of staff through social media, they should be reported to the headteacher.
- Members of staff should avoid identifying themselves as an employee of Silver Linings School on social media. Members of staff must not post content online which is damaging to the school or any of its staff or pupils.
- Where teachers or members of staff use social media in a personal capacity, they should make it clear that their views are personal.
- Teachers or members of staff must not post any information which could identify a pupil, class or the school.
- Members of staff should not post anonymously or under an alias to evade the guidance given in this policy.
- Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal.
- Members of staff should be aware that if their out-of-work activity brings Silver Lining School into disrepute, disciplinary action will be taken.
- Members of staff should regularly check their online presence for negative content.
- Attempts to bully, coerce or manipulate members of the school community, via social media, by teachers and members of staff will be dealt with as a disciplinary matter.
- Members of staff should not leave a computer or other device logged in when away from their desk.

Social Media Use – Pupils and Parents/Carers

- Pupils are responsible for following the school rules and will be expected to follow requests from teachers.
- Pupils may not access social media during lesson time, unless it is part of a curriculum activity.
- Breaches of this policy by pupils will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to exclusion.
- Pupils and parents/carers must not attempt to "friend" or otherwise contact members of staff through social media. If attempts to contact members of staff through social media are made, they will be reported to the headteacher.
- Pupils and parents/carers should not post anonymously or under an alias to evade the guidance given in this policy.
- Pupils and parents/carers must not post content online which is damaging to the school

or any of its staff or pupils.

- Pupils at Silver Linings School must not sign up to social media sites that have an age restriction above the pupil's age.
- If inappropriate content is accessed online on school premises, it must be reported to a teacher.
- Any offensive or inappropriate comments pupil's post about Silver Linings School will be resolved by the use of the school behaviour policy.
- If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
- Parents/Carers are encouraged to comment or post appropriately about Silver Linings School. In the event of any offensive or inappropriate comments being made, the School will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the Silver Linings School's complaints procedures.

Technical – Infrastructure/Equipment, Filtering and Monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people in the above sections will be effective in carrying out their online safety responsibilities.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- The "master/administrator" passwords for the school ICT system, must be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe).
- software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing Classroom Cloud. Content lists are regularly updated and internet use is logged and regularly monitored.
- The school has provided enhanced/differentiated user-level filtering.
- An appropriate system is in place for users to report any actual / potential technical incident/security breach to the relevant person.
- An agreement is in place regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on school devices that

may be used out of school.-see staff acceptable use policy and Individual user agreements for Children.

- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of online and video images

The development of online imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing online images on the internet. Such images may provide avenues for cyberbullying to take place. Online images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using online images, staff should inform and educate 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.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and online images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the online/video images.
- Staff and volunteers are allowed to take online/video images to support educational aims using school cameras/tablets, but must follow school policies concerning the sharing, distribution and publication of those images. The personal equipment of staff should not be used for such purposes.
- Care should be taken when taking online/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website.
- Staff and pupils must not publish online, copyrighted images on the school's website or social media pages.

Data Protection
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and GDPR 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

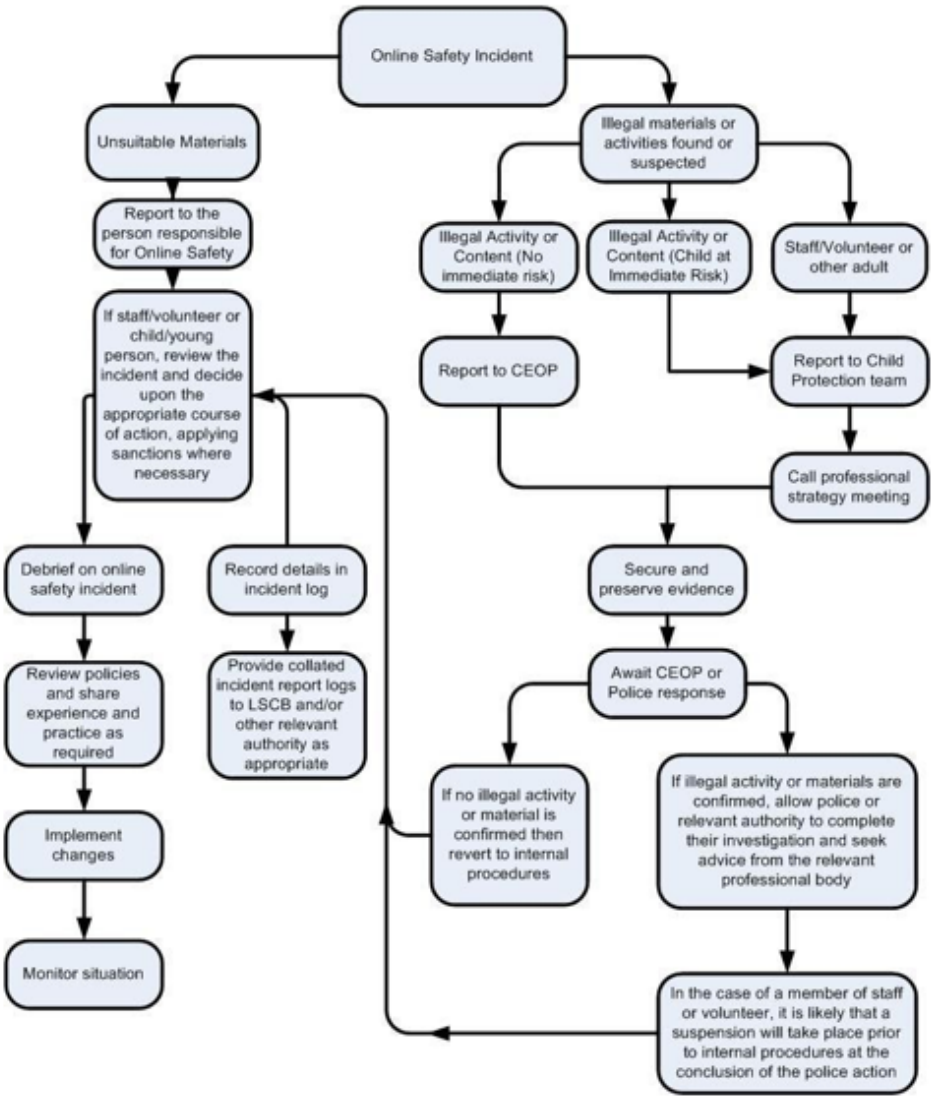
- Take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse, at all times.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device once it has been transferred or its use is complete for these communications.
- website and only official email addresses should be used to identify members of staff.

Responding to issues of misuse
This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents
If there is any suspicion that the website(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) for responding to online safety incidents and report immediately to the police**.**



Other Incidents

It is hoped that all members of the school community will be responsible users of online technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
- once this has been completed and fully investigated, the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority
    - Police involvement and/or action
    - If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately.

Other instances to report to the police would include:

- -incidents of 'grooming' behaviour
- -the sending of obscene materials to a child
- -adult material which potentially breaches the Obscene Publications Act
- -criminally racist material
- -other criminal conduct, activity or materials.

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.
It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed information should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

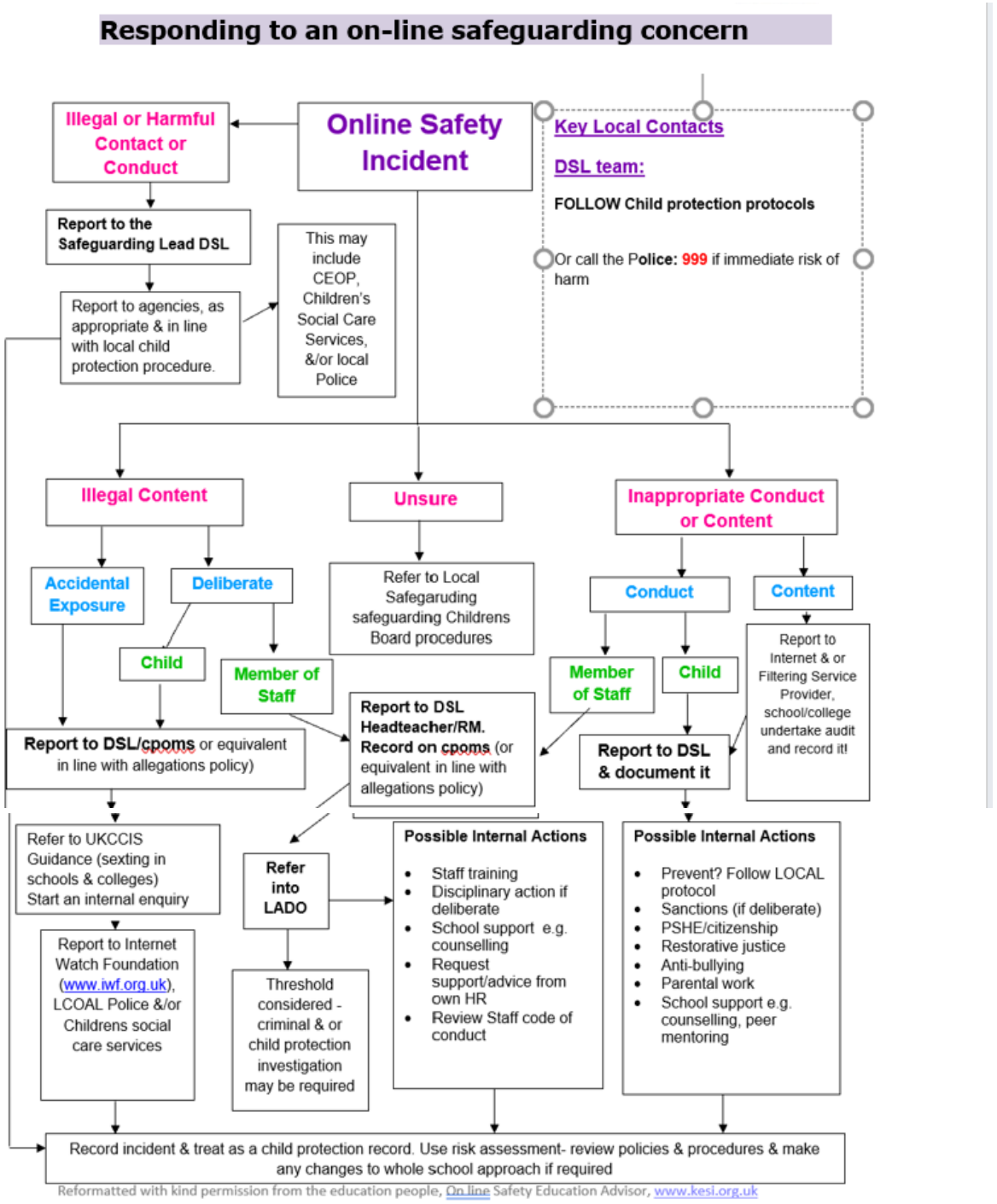
Training

- It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:
- A planned program of formal online safety training will be made available to staff.

This will be regularly updated and reinforced.

- All new staff should receive online safety training as part of their induction program, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.

APPRENDIX 1



Silver Linings School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all pupils feel safe and fulfil their personal emotional and academic potential.			
Review due:	Aug 2025	**Reviewed by:**	Julia Whitesides
Date reviewed:	Sept 2023	**Policy:**	Online & social media

Appendix 2

Appropriate Internet use by pupils/students at Silver Linings School

- I will ask permission from an adult before using the Internet
- I will use computers and tablets safely.
- I will not look for websites that I know I'm not allowed to see.
- If I see anything that I know is wrong I will tell an adult straight away.
- I will not download anything without permission from an adult
- I will not use memory sticks on school computers
- I will ask an adult before sending emails or messages.
- I will be polite and respect others when using the Internet.
- I will not give out any personal information over the Internet.
- I will not share my login details with others.
- I understand that the school or my parents may check my computer files and check what I am doing.