E safety policy

August 2025

SKERN

Table of Contents

SKERN

SKERN

Policy

Skern is committed to safeguarding adults and children's agenda and believes that the welfare of people is a priority and at all times people using Skern's services have a right to feel safe and protected from any situation or practice that results in them being harmed or at risk of harm.

Policy aims

The purpose of the online safety policy is to:

- Safeguard and protect all members of the community online.
- Identify approaches to raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

Online safety has a high emphasis on a competent well-established workforce, up to date policies and procedures, robust governance arrangements and collaborative practices. Types of online risk usually fall under one of three categories:

- **Contact:** Contact from someone online who may wish to bully or abuse another person. This could also include online grooming, online harassment or activities of a commercial nature, including tracking and harvesting personal information.
- **Content:** Inappropriate material available online including: adverts, spam, sponsorship, personal info, violent or hateful content, pornographic or unwelcome sexual content, biassed materials, racist materials, and misleading information or advice.
- **Conduct:** The person may be the perpetrator of activities including: illegal downloading, hacking, gambling, financial scams, bullying or harassing another child. They might create and upload inappropriate material or provide misleading information or advice.

Policy scope

- Skern believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all are protected from potential harm online.

- Skern identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- This policy applies to all staff including the directors, delivery staff, support staff, external contractors, visitors, apprentices, volunteers and other individuals who work for, or provide services on behalf of Skern (collectively referred to as 'staff 'in this policy) as well as adults, young people and children using our sites/services and parents/carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where children, young people, adults at risk, staff or other individuals have been provided with company issued devices for use, such as work laptops, tablets or mobile phones.

Links with other policies and practices

This policy links with a number of other policies, practices and action plans including:

- Safeguarding Policy and Procedures
- Code of Conduct
- Prevent and Radicalisation Policy
- Data Protection Act 2018
- General Data Protection Regulations
- Online Safety Act 2023

Monitoring and review

- Skern Management will review this policy annually.
- The policy will also be revised following any national or local policy requirements, any child or adult protection concerns or any changes to the technical infrastructure.
- We will continue to apply restrictions to the material users' access.
- To ensure they have oversight of online safety, the Head of Safeguarding will be informed of online safety concerns, as appropriate.
- Online safety incidents will be recorded on Patronus, including outcomes.
- Any issues identified will be incorporated into future action planning.

Defining online abuse

"Online abuse is any type of abuse that happens on the web, whether through social networks, playing online games or using mobile phones" (NSPCC, 2019).

Hidden harms – types of online abuse may include:

- Cyberbullying
- Emotional abuse
- Grooming
- Sexting
- Sexual abuse
- Sexual exploitation

The types, patterns and different circumstances of significant harm and abuse should be considered within the categories identified for children in the Children Act 1989 / 2004. These are:

- Neglect
- Sexual Abuse
- Physical Abuse
- Emotional Abuse

Technology can facilitate a world of learning and development in addition to helping yield a range of opportunities. However, the stark reality is that it can also present a window to potential and actual harm and abuse. It can elicit and support an array of illegal abusive behaviours including, but not limited to:

- Harassment
- Stalking
- Threatening behaviour
- Creating or sharing child sexual abuse material
- Inciting a child to sexual activity
- Sexual exploitation
- Grooming
- Sexual communication with a child
- Causing a child to view images or watch videos of sexual act

Roles and responsibilities

- Skern has designated Safeguarding Leads for each Education and Residential parts of the business (See Safeguarding Policy) They have responsibility for Safeguarding, Prevent and E-Safety.
- Skern recognises that all members of the organisation have important roles and responsibilities to play with regards to online safety.
- Skern has a number of Designated Safeguarding Leads (DSLs) who have a collective responsibility to support the awareness raising via the staff training and those in their areas of the business.
- DSL has lead responsibility for the coordination and management of any E-Safety safeguarding concerns.

Safeguarding quarterly meetings

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a Code of conduct and/or an Acceptable Use Policy (AUP), which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering systems are in place.
- Work with technical staff to monitor the safety and security of Skern's systems and networks.
- Ensure that online safety is embedded within the company culture, which enables all to understand online safety.
- Support the Designated Safeguarding Leads by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for Skern's community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.

Designated Safeguarding Lead (DSL):

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Keep up to date with current research, legislation and trends regarding online safety and communicate to all staff, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to all staff and visitors to residential sites through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of Skern's safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends and use this data to update and influence policies and procedures.
- Report online safety concerns, as appropriate via Patronus.

It is the responsibility of all members of staff to:

- Contribute to the development of E-Safety Policies.
- Read and adhere to the E-Safety Policy, Code of conduct and AUPs.
- Take responsibility for the security of company systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Have an awareness of a range of online safety issues and how they may be experienced by the individuals in their care.
- Identify online safety concerns and take appropriate action by following the safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

It is the responsibility of staff managing the technical environment to:

- Provide technical support and guidance to the company in the technical implementation of online safety procedures and controls.
- Implement appropriate security measures (including password policies and encryption) to ensure that IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that filtering is applied and updated on a regular basis.
- Report any filtering breaches to the Directors, where a breach need escalating, appropriate agencies such as the Internet Watch Foundation, the Police, and/or Child Exploitation and Online Protection will be engaged.
- Ensure that any safeguarding concerns, identified through filtering breaches are reported to the DSL, in accordance with the Safeguarding Policy and Procedures.

It is the responsibility of all visiting guests to:

- Read and adhere to the company Code of Conduct and AUP.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

It is the responsibility of party leaders and their teams to:

- Read the Code of Conduct, E-Safety guidance and relevant AUPs and encourage their children, young people and adults to adhere to them.
- Support Skern in its online safety approach.
- Role model safe and appropriate use of technology and social media.
- Seek help and support, or other appropriate agencies, if they or their child, young people or adults at risk encounter risk or concerns online.

Education and engagement approaches

Skern will establish and embed a progressive E-Safety awareness raising programme, to raise awareness and promote safe and responsible internet use amongst all by:

- Ensuring awareness raising regarding safe and responsible use precedes internet access.
- Reinforcing online safety messages across Skern sites including use of Skern systems and personal technology.

We will also specifically support leaners in STS by ensuring that E-safety and expectations around online learning is covered within induction period, ideally on first day of learning. Topics to include are: **Understanding Online Risks, Responsible Online Behaviour, Responding to Online Harm, Digital Literacy, Staying Safe Online, Keeping Children Safe in Education, Regular Updates, Online safety and social media, Cyberbullying, Online grooming, Inappropriate content, Digital footprint and reputation, Privacy and security.**

Vulnerable individuals

- Skern is aware that some individuals are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss together with adults at risk for similar circumstances.
- Skern will ensure that differentiated and ability appropriate online safety awareness, access and support is provided to those individuals (which is age appropriate).

Training and engagement with staff

Skern will:

- Provide the Online Safety Policy with all staff as part of their induction.
- Ensure that Online Safety is covered as a part of staff training.
- Continue to remind and educate staff to behave professionally and in accordance with the policies when accessing company systems and devices.
- Make staff aware that their online conduct outside of Skern working time, including personal use of social media, could have an impact on their professional role and reputation within the business.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting children, young people, adults at risk, colleagues or other members of the Skern community.

Reducing online risks

Skern recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Ensure that appropriate filtering is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via accompany computer or device.

All members of the company are made aware of the expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the Code of Conduct and highlighted through a variety of awareness raising approaches.

Safer use of technology

Educational use

Skern uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Internal platforms
- Emails
- Games consoles and other games-based technologies
- Digital cameras, webcams and video cameras

Al company owned devices will be used in accordance with IT AUP and with appropriate safety and security measures in place. Members of staff will always evaluate websites, tools and apps fully before use in any setting. Skern will ensure that the use of internet derived materials, by staff and visitors, complies with copyright law and acknowledges the source of information. Supervision of children, young people and adults at risk will be appropriate to their age and vulnerability.

Managing internet access

- Apply appropriate technical and procedural controls to ensure that the Skern infrastructure/system is secure and not open to misuse or malicious attack while allowing productivity and learning opportunities to be maximised.
- All staff will read, adhere and promote the best use of IT in accordance with the Code of Conduct and IT Acceptable Use Agreements policies.

Filtering and monitoring

Decision making

- Skern Management have ensured that appropriate filtering is in place, to limit exposure to online risks.
- Changes to the filtering approach will be risk assessed by staff with technical experience (often outsourced) and, where appropriate, with consent from the company; all changes to the filtering policy are logged and recorded.
- All members of staff are aware that they cannot rely on filtering alone to safeguard; effective management and regular awareness raising about safe and responsible use is essential.

Filtering

- Skern operates on a single network, with a connection to the internet that is managed by a firewall. This firewall inspects internet traffic to block malware and many other threats. The firewall also blocks access to and from harmful and malicious websites. The firewall rules and access is managed by the IT Department at Argon. Additional Content Filtering is powered by Cisco Talos which is Cisco's Security Intelligence and Research Group. They constantly track a broad set of attributes to evaluate conclusions about a given website. This allows Skern to proactively filter, or block websites visited by users on the Network. The firewall also provides the IT team with monitoring, analysis, and reporting on activity by users on the Network. All

members of staff are aware that they cannot rely on filtering and Cyber Security Awareness training is essential.

- Skern uses appropriate filtering systems which block sites which can be categorised as: CSA content, pornography, racial hatred, extremist and terrorist content, gaming and sites of an illegal nature.
- Skern tests the effectiveness of the filtering system in December on an annual basis.
- Skern will ensure that the filtering system will not 'overblock' the usage.

Dealing with filtering breaches

Skern has a clear procedure for reporting filtering breaches.

Step 1

If individuals discover unsuitable sites, they will be required to turn off the monitor/screen and report the concern immediately to a member of staff.

Step 2

The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead.

Step 3

The breach will be recorded and escalated as appropriate.

Step 4

Parents/carer, party leaders will be informed of filtering breaches involving their child/adult.

Step 5

Any material that Skern believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, Police.

Monitoring

- Skern strictly prohibits the sharing of networks or devices with children and young people who visit their sites. It is essential to note that Skern does not operate any monitoring systems.

Security and management of information systems

Skern takes appropriate steps to ensure the security of our information systems.

- Virus protection being updated regularly.

- Not using portable media without specific permission; portable media will be checked by an anti-virus/malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on the Skern network.
- The appropriate use of user logins and passwords to access the Skern network. (Specific user logins and passwords will be enforced for all).
- All users are expected to log off or lock their screens/ devices if systems are unattended.

Password policy

All members of staff will have their own unique username and private passwords for access; members of staff are responsible for keeping their password private.

We require all users to:

- Use strong passwords for access into our system.
- 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.

Managing the safety of the group's websites

- Skern will ensure that information posted on our websites meet the requirements as identified by the Department for Education (DfE) and in line with OFSTED.
- Skern will ensure that our websites comply with guidelines for publications including accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- No personal information will be published on our websites; the contact details on the websites will be the company address, email, and telephone number.
- The administrator accounts for the Group's websites will be secured with an appropriately strong password.
- Skern will post appropriate information about safeguarding, including policies, on the Group's websites for members of the community.

Managing email

Access to Skern email systems will always take place in accordance with Data Protection legislation and in line with other policies, including confidentiality and Code of conduct.

- 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.
- Skern email addresses and other official contact details will not be used for setting up personal social media accounts.

Members of the Skern community will immediately inform the DSL if they receive offensive communications, and this will be recorded in the safeguarding files/records.

Staff

The use of personal email addresses by staff for any official Skern business is not permitted except where required for business communications and an official Skern email address was not provided.

All members of staff who are provided with a specific company email address, to use for all official communication.

Use of video conferencing and/or webcams

Skern recognises 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.
- Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
- Videoconferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

Users

- Party leaders or responsible individuals, consent will be obtained prior to any child, young person or adult at risk taking part in videoconferencing activities.
- Videoconferencing will be supervised appropriately, according to age and ability.
- Videoconferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote-control pages.
- The unique login and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

Content

- When recording a videoconference, it should be made clear to all parties at the start of the conference and 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, Skern will check that recording is permitted to avoid infringing the third-party intellectual property rights.
- Skern will establish dialogue with other conference participants before taking part in a videoconference; staff will check that the material they are delivering is appropriate for the class.

Social Media

The expectations' regarding safe and responsible use of social media applies to all members of Skern.

The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chat rooms and instant messenger.

All members of the Skern are expected to engage in social media in a positive, safe and responsible manner, at all times.

All members of Skern are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

Inappropriate or excessive use of social media during work hours or whilst using Skern devices may result in disciplinary or legal action and/or removal of internet facilities.

Concerns regarding the online conduct of any member of Skern on social media, should be reported to the DSL and will be managed in accordance with our Anti-bullying, Allegations against staff, Code of conduct and Safeguarding policies.

Staff personal use of social media

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the Code of conduct.

Reputation

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within Skern. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

- Setting the privacy levels of their personal sites as strictly as they can.
- Being aware of location sharing services.
- Opting out of public listings on social networking sites.
- Logging out of accounts after use.
- Keeping passwords safe and confidential.
- Ensuring staff do not represent their personal views as that of Skern.

Members of staff are encouraged not to identify themselves as employees of Skern on their personal social networking accounts. This excludes professional networking sites such as LinkedIn, however employees are reminded that activity on social media sites which is harmful to Skern is not permitted.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with Skern policies and the wider professional and legal framework.

Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.

Members of staff will notify the DSL immediately if they consider that any content shared on social media sites conflicts with their role in Skern.

Communicating with visitors and party leaders

All members of staff are advised not to communicate with or add as ‘friends’ any current or past guests, or current or past guest’s family members via any personal social media sites, applications or profiles.

- Any pre-existing relationships or exceptions that may compromise this will be discussed with the DSL.

- If ongoing contact with guests is required once they have concluded their time at Skern, members of staff will be expected to use existing corporate networks and official Skern provided communication tools.

Staff will not use personal social media accounts to make contact with guests or parents, nor should any contact be accepted. Any communication from guests and parents received on personal social media accounts will be reported to the DSL.

Guests' personal use of social media

Any concerns regarding children, young people or adults at risk use of social media, whilst with Skern, will be dealt with in accordance with existing policies including Safeguarding and Anti-bullying policy. Concerns will also be raised with parents, party leaders as appropriate, particularly when concerning underage use of social media sites or tools.

E-safety advice for guests and learners will include:

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/protected.

- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications and report concerns both within Skern and externally.

Official use of social media

Skern has a range of official social media channels.

The official use of social media sites, by Skern, only takes place with clear educational or community engagement objectives, with specific intended outcomes.

Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.

- Staff use Skern provided email addresses to register for and manage any official Skern social media channels.
- Official social media sites are suitably protected and, where possible, run and/or linked to/from the relevant Skern website.
- Public communications on behalf of Skern will, where appropriate and possible, be read and agreed by at least one other colleague.

Official social media use will be conducted in line with existing policies, including: Anti-bullying, Image use, Data protection, Confidentiality, Code of Conduct and Safeguarding procedures.

- All communication on official social media platforms will be clear, transparent and open to scrutiny.

Party Leaders, parents and guests will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

- Social media tools which have been risk assessed and approved as suitable for educational purposes will be used.

Parents and party leaders will be informed of any official social media use with guests and written parental consent will be obtained, as required.

Staff expectations

Members of staff who follow and/or like the Skern social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

If members of staff are participating in online social media activity as part of their capacity as an employee of SKern, they will:

- Be professional at all times and aware that they are an ambassador for the organisation.
- Disclose their official role and/or position but make it clear that they do not necessarily speak on behalf of Skern.
- Be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Always act within the legal frameworks they would adhere to within the workplace, including: Libel, Defamation, Confidentiality, Copyright, Data protection and Equalities laws.
- Ensure that they have appropriate written consent before posting images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of Skern unless they are authorised to do so.
- Not engage with any direct or private messaging with current, or past, guests, parents and carers.
- Inform their Designated Safeguarding Lead of any concerns, such as criticism, inappropriate content or contact from guests.

Staff use of personal devices and mobile phones

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant Skern policy and procedures, such as: Confidentiality, Safeguarding, Data Security and Acceptable Use.
Staff will be advised to:

- Only take mobile phones onto sessions if essential for emergency communication.
- Keep mobile phones and personal devices in a safe and secure place during instruction time. For example, make sure it doesn't fall out from your pocket during delivery.
- Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times where possible.
- Ensure that Bluetooth or other forms of communication (such as 'Airdrop') are hidden or disabled during activity times if carrying the phone with you.
- Do not use personal devices during activity periods unless it's necessary for the instruction or safety purposes.
- Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

Members of staff are not permitted to use their own personal phones or devices for contacting guests or parents and carers.

Any pre-existing relationships, which could undermine this, will be discussed with the Designated Safeguarding Lead. Staff will not use personal devices, such as mobile phones, tablets or cameras to take photos or videos of guests and will only use work provided equipment for this purpose.

If a member of staff breaches the Skern policy, action will be taken in line with the staff allegations process.

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or has committed a criminal offence, the police will be contacted.

Guests' use of personal devices and mobile phones

Policy on the possession and use of mobile phones and tablets by guests attending as part of an organised school, youth or faith group is the responsibility of that party leaders to determine and implement; however they must adhere to the Code of Conduct.

For guests attending a program such as HAF, the decision to bring a mobile phone or tablet ultimately lies with their Parent/Guardian, but we discourage them from being brought along.

For those who do choose to bring a mobile phone or tablet the following rules apply:

- Not to be used in dormitories.
- Not to be used during activities.
- Not to be used during meal times whilst in the dining hall.
- Taking photographs/media of other campers or staff is not permitted without their permission.
- Not to be used to look at or post inappropriate or offensive content.

These rules are included in the pre-visit documentation and Code of conduct. There will also be information for guests who may have upsetting online or text experiences while visiting prior to or after a visit and need help or advice.

To help parents decide whether to let their child take a phone, we make them aware that we are unable to monitor their child's use of their phone at all times. Access to the internet is outside our control when it is done through phone networks, and we are unable to police what content is being accessed. A parent's decision to allow their child to take a phone is as much about their trust in their child to stick to the rules as it is about our ability to enforce them.

Where phones or tablets are brought along, we may offer a facility for them to be handed in for safekeeping, then re issued for agreed periods of use.

Guests will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

Skern expects guest's personal devices and mobile phones to remain in their accommodation until activities have concluded.

If a guest needs to contact his/her parents or carers, they will be allowed to use an company phone.

- Skern may confiscate a guest's mobile phone or device if they believe it is being used to contravene the Code of conduct, Bullying policy or could contain youth produced sexual imagery (sexting).
- Guests' mobile phones or devices may be searched by a DSL, with the consent of the guest or a parent/carer. Content may be deleted or requested to be deleted, if it contravenes Skern policies.
- Mobile phones and devices that have been confiscated will be released to parents or carers. If there is suspicion that material on a guest's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

Visitors' use of personal devices and mobile phones

- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the Code of Conduct and other associated policies, such as: Anti-bullying, Code of conduct, Safeguarding and Image use.
- Skern will ensure appropriate signage and information is displayed/provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of Skern policy.

Officially provided mobile phones and devices

- Members of staff may be issued with a work mobile phone number.
- Skern mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- Skern mobile phones and devices will always be used in accordance with the Code of Conduct and other relevant policies.

Responding to online safety incidents and concerns

All members of Skern will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery, cyberbullying and illegal content.

All members of the community must respect confidentiality and the need to follow the official Skern procedures for reporting concerns.

- Learners, guests parents and staff will be informed of the complaints procedure and staff will be made aware of the whistleblowing procedure.
- Skern requires staff, parents, carers, learners and guests to work in partnership to resolve online safety issues.
- After any enquiries are completed, Skern will debrief, identify lessons learnt and implement in a policy.
- If Skern staff are unsure how to proceed with an incident or concern, the DSL will seek advice from the MASH.
- Where there is suspicion that illegal activity has taken place Skern will contact the MASH/101, or 999 if there is immediate danger or risk of harm.

Concerns about pupils' welfare

- The DSL will be informed of any online safety incidents involving safeguarding, child or adult protection concerns.
- The DSL will record these issues in line with the Safeguarding policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Local Safeguarding Board thresholds and procedures.
- Skern or the relevant group/party leader will inform parents and carers of any incidents or concerns involving their child, as and when required.

Staff misuse

- Any complaint about staff misuse will be referred to the Designated Safeguarding Lead according to the allegations procedures.
- Any allegations regarding a member of staff's online conduct that meet the threshold will be discussed with the LADO (Local Authority Designated Officer).

Procedures for responding to specific online incidents or concerns

Youth produced sexual imagery or "sexting"

- Skern recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- Skern will follow the advice as set out in national guidance.
- Skern will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches. Skern will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

Dealing with 'sexting'

If Skern are made aware of an incident involving the creation or distribution of youth produced sexual imagery, they will:

Step 1
Act in accordance with safeguarding policies and the relevant Local Safeguarding Children's Board procedures.

Step 2
Immediately notify the Designated Safeguarding Lead

Step 3

Store the device securely. If an indecent image has been taken or shared on the Skern network or devices, Skern will take action to block access to all users and isolate the image.

Step 4
Carry out a risk assessment which considers any vulnerability of children, young people and adults at risk involved; including carrying out relevant checks with other agencies.

Step 5
Inform parents and carers, if appropriate, about the incident and how it is being managed.

Step 6
Make a referral to children's social care care/MASH and/or the Police, as appropriate.

Step 7
Provide the necessary safeguards and support for children, young people and adults at risk, such as offering counselling or pastoral support.

Step 8
Images will only be deleted once Skern has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.

Step 9
Review the handling of any incidents to ensure that best practice was implemented; the SAG will also review and update any management procedures, where necessary.

Skern will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off Skern premises, or personal equipment.

Skern will not:

- View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to

do so. (In this case, the image will only be viewed by the Designated Safeguarding Lead and their justification for viewing the image will be clearly documented).

- Send, share, save or make copies of content suspected to be an indecent image of children (i.e. youth produced sexual imagery) and will not allow or request guests to do so.

Online child sexual abuse and exploitation

Skern will ensure that all members of staff are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

Skern recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL.

Skern will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate methods of communication for guests, party leaders and parents.

Skern will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.

Dealing with online child sexual abuse and exploitation

If Skern is made aware of incident involving online sexual abuse of a child, young person or adult at risk they will follow protocol as detailed re “sexting”.

If Skern is unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the MASH and/or respective regional Police.

If Skern is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the MASH and respective Police by the DSL.

If individuals outside Skern are believed to have been targeted also, Skern will seek the support from Police and/or MASH first to ensure that potential investigations are not compromised.

Indecent images of children (IIOC)

Skern will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

Skern will take action regarding IIOC on their equipment and/or personal equipment, even if access took place off site.

Skern will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

If Skern is unclear if a criminal offence has been committed, the DSL will obtain advice immediately through their local Police and/or Multi Agency Safeguarding Hub.

If made aware of IIOC, Skern will:

- Act in accordance with the Skern Safeguarding policy and operational manual and the relevant local Safeguarding Child Board procedures.
- Immediately notify the DSL.
- Store any devices involved securely.
- Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), MASH/ Police and or the LADO.

If made aware that a member of staff, child, young person or adult at risk has been inadvertently exposed to indecent images of children whilst using the internet, Skern will:

- Ensure that the Designated Safeguard Lead is informed.
- Ensure that the URLs (web page addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to party leaders, parents and carers.

If made aware that indecent images of children have been found on Skern devices, they will:

- Ensure that the DSL is informed.
- Ensure that the URLs (web page addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
- Identify where all copies of the images are held.
- Inform the police via 101 (999 if there is an immediate risk of harm) and children's social care (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents and carers.

If made aware that a member of staff is in possession of indecent images of children on Skern devices, Skern will:

- Ensure that the DSL is informed.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with Skern allegations procedures.
- Quarantine any devices until police advice has been sought.

Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at Skern. Full details of how Skern will respond to cyberbullying are set out in the Anti-bullying policy and Code of conduct.

Online hate

Online hate content, directed towards or posted by specific members of the community will not be tolerated at Skern and will be responded to in line with existing policies, including Anti-bullying and Code of Conduct. All members of the community will be advised to report online hate in accordance with relevant policies and procedures. The Police will be contacted if a criminal offence is suspected.

If is unclear on how to respond, or whether a criminal offence has been committed, the DSL will obtain advice through the MASH and/or local Police as identified in Local Arrangements Documents.

Online radicalisation and extremism

Skern will take all reasonable precautions to ensure that children, young people and adults at risk are safe from terrorist and extremist material when accessing the internet through its systems.

If anyone is concerned that a child, young person or adult at risk or any other member of the company may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately, and action will be taken in line with Safeguarding/Prevent policies.

See also Prevent and Radicalisation policy and Safeguarding policy and procedures.

Useful links

National links and resources:

Action Fraud: www.actionfraud.police.uk

CEOP www.ceop.police.uk

Think UK now: www.thinkuknow.co.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

SKERN

Internet Watch Foundation (IWF): www.iwf.org.uk

Lucy Faithfull Foundation: www.lucyfaithfull.org

NSPCC: www.nspcc.org.uk/onlinesafety

ChildLine: www.childline.org.uk

Net Aware: www.net-aware.org.uk

The Marie Collins Foundation: www.mariecollinsfoundation.org.uk

UK Safer Internet Centre: www.saferinternet.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

Sexual violence and sexual harassment between children in schools and colleges 2021:
https://www.gov.uk/government/publications/sexual-violence-and-sexual-harassment-betw een-children-in-schools-and-colleges

Keeping Children Safe in Education 2023:

Keeping children safe in education - GOV.UK (www.gov.uk)