**Saplings Online Safety (e-Safety) Policy**

Saplings believe that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world when using technology such as computers, mobile phones, or games consoles....

Saplings identify that the internet and information communication technologies are an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.

Saplings have a duty to provide the school community with quality Internet access to raise education standards, promote pupil achievement, support the professional work of staff and enhance the schools management functions.

Saplings also identify that with this there is a clear duty to ensure that children are protected from potential harm online.

**The purpose of Sapling's online safety policy is to:**

* Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that Saplings is a safe and secure environment.
* Safeguard and protect all members of the Saplings community online.
* Raise awareness with all members of the Saplings community regarding the potential risks as well as benefits of technology.
* To enable all staff to work safely and responsibly to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
* Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

 This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as ‘staff‘ in this policy) as well as children and parents/carers.

 This policy applies to all access to the internet and use of information communication devices including personal devices or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptop or mobile phone.

This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, image use, Acceptable Use Policies, confidentiality, screening, searching and confiscation and relevant curriculum policies including computing, Personal Social Health and Education (PSHE), Citizenship and Sex and Relationships education (SRE).

Saplings online safety policy has been written by the school, involving staff, pupils, and parents/carers.

The policy has been approved and agreed upon by the Leadership/Management Team

 Saplings have appointed a member of the Management team to take the lead responsibility for online safety (e-safety).

Saplings online safety (e-Safety) Policy and its implementation will be reviewed at least annually or sooner if required. The School Online safety (e-Safety) Coordinator is Jo Warwick and Casey Parker

 The School Designated Safeguarding Lead (DSL) is Jo Warwick and Casey Parker

All members of school/setting communities have an essential role to play in ensuring the safety and wellbeing of others, both on and offline. It is important that all members of the community are aware of these roles and responsibilities and how to access and seek support and guidance.

**The key responsibilities of the Saplings management and leadership team are:**

* Developing, owning and promoting the online safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the school community.
* Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
* Supporting online safety (e-Safety) leads to the development of an online safety culture within the setting.
* Ensuring there are appropriate and up-to-date policies and procedures regarding online safety.
* To ensure that suitable, age-appropriate, and relevant filtering is in place to protect children from inappropriate content (including extremist material) to meet the needs of the school community and ensure that the filtering and school network system is actively monitored.
* Ensuring all members of staff receive regular, up-to-date, and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
* Ensuring that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
* Making appropriate resources available to support the development of an online safety culture.
* Taking responsibility for online safety incidents and liaising with external agencies as appropriate.
* Receiving and regularly reviewing online safety incident logs and using them to inform and shape future practice.
* Ensuring there are robust reporting channels for the Saplings 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, including ensuring the safe and responsible use of devices.
* To work with and support technical staff in monitoring the safety and security of Saplings systems and networks.
* To ensure a member of the management team is identified with a lead responsibility for supporting online safety.
* To ensure that the Designated Safeguarding Lead (DSL) works in partnership with the online safety (e-Safety) lead.

**The key responsibilities of the designated safeguarding/online safety (e-Safety) lead are**

Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate.

Keeping up to date with current research, legislation, and trends.

Coordinating participation in local and national events to promote positive online behaviour, e.g., Safer Internet Day.

Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.

Work with the Saplings lead for data protection and data security to ensure that practice is in line with legislation.

Maintaining an online safety incident/action log to record incidents and actions taken as part of the Saplings safeguarding recording structures and mechanisms.

Monitor the Saplings online safety incidents to identify gaps/trends and update the education response to reflect the need and report to the school management team, and other agencies as appropriate.

 Liaising with the local authority and other local and national bodies as appropriate.

Reviewing and updating online safety policies, Acceptable Use Policies (AUPs), and other procedures on a regular basis (at least annually) with stakeholder input.

Ensuring that online safety is integrated with other appropriate Sapling's policies and procedures.

**The key responsibilities for all members of staff are**

Contributing to the development of online safety policies.

Reading the Saplings Acceptable Use Policies (AUPs) and adhering to them.

Taking responsibility for the security of Saplings systems and data.

Having an awareness of online safety issues, and how they relate to the children in their care.

Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities rather than focusing on negatives.

Embedding online safety education in curriculum delivery wherever possible.

Identifying individuals of concern and taking appropriate action by working with the designated safeguarding lead.

Knowing when and how to escalate online safety issues, internally and externally.

Being able to signpost to appropriate support available for online safety issues, internally and externally.

Maintaining a professional level of conduct in their personal use of technology, both on and off-site.

Taking personal responsibility for professional development in this area

**The key responsibilities of parents and carers are:**

Reading the Saplings Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.

Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.

Role modelling safe and appropriate uses of new and emerging technology.

Identifying changes in behaviour that could indicate that their child is at risk of harm online.

Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.

Contributing to the development of the Saplings online safety policies.

Using school systems, such as learning platforms, and other network resources, safely and appropriately.

Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies

Saplings will ensure that all images are used in accordance with the school image use policy.

In line with the Saplings image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

**Staff use of personal devices and mobile phones**

Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-exiting relationships which could compromise this must be discussed with leaders/managers.

Staff will not use personal devices such as mobile phones, tablets, or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.

Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.

Staff will ensure that any content bought on-site via mobile phones and personal devices is compatible with their professional role and expectations.

If a member of staff breaches the Saplings policy, then disciplinary action will be taken.

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offense then the police will be contacted, and allegations will be responded to following the allegations management policy.

**Visitor's use of personal devices and mobile phones**

Parents/carers and visitors must use mobile phones and personal devices in accordance with the Saplings policy.

Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the Saplings image use policy.

Saplings will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.

Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors

**Reducing online risks**

Saplings are aware that the Internet is a constantly changing environment with new apps, tools, devices, sites, and materials emerging at a rapid pace.

Emerging technologies will be examined for educational benefit and the Saplings leadership team will ensure that appropriate risk assessments are carried out before use in Saplings is allowed.

Saplings will ensure that appropriate filtering systems are in place to prevent staff and pupils from accessing unsuitable or illegal content. Schools should include appropriate details about the systems in place.

Saplings will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer or device.

Saplings will audit technology use to establish if the online safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.

Methods to identify, assess and minimize online risks will be reviewed regularly by Saplings leadership team.

Filtering decisions, internet access and device use by pupils and staff will be reviewed regularly by the Saplings management team.

**Management of applications (apps) used to record children’s progress**

The manager is ultimately responsible for the security of any data or images held of children.

Apps/systems which store personal data will be risk assessed prior to use.

Personal staff mobile phones or devices will not be used for any apps which record and store children’s personal details, attainment or photographs.

Only Saplings issued devices will be used for apps that record and store children’s personal details, attainment or photographs.

Devices will be appropriately encrypted if taken off-site to prevent a data security breach in the event of loss or theft.

Staff and parents/carers will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.

 **Responding to Online Incidents and Concerns**

All members of Saplings community will be informed about the procedure for reporting online safety (e-Safety) concerns (such as breaches of filtering, cyberbullying, illegal content etc.).

The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.

The Designated Safeguarding Lead (DSL) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.

Complaints about Internet misuse will be dealt with under the Saplings complaints procedure.

Complaints about online bullying will be dealt with under the Saplings anti-bullying policy and procedure

Any complaint about staff misuse will be referred to the managers

Any allegations against a member of staff’s online conduct will be discussed with the LADO (Local Authority Designated Officer).

Pupils, parents and staff will be informed of the Saplings complaints procedure.

Staff will be informed of the complaints and whistleblowing procedure.

All members of the Saplings community will need to be aware of the importance of confidentiality and the need to follow the official Saplings procedures for reporting concerns.

All members of the Saplings community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images, or videos online which cause harm, distress, or offense to any other members of the apling community.

Saplings will manage online safety (e-Safety) incidents in accordance with the school discipline/behaviour policy where appropriate.

Saplings will inform parents/carers of any incidents of concerns as and when required.

After any investigations are completed, Saplings will debrief, identify lessons learnt and implement any changes as required.

Where there is cause for concern or fear that illegal activity has taken place or is taking place then Saplings will contact the Education Safeguards Team or Kent Police via 999 if there is immediate danger or risk of harm.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.

If Saplings is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.

If an incident of concern needs to be passed beyond Saplings, then the concern will be escalated to the Education Safeguarding Team to communicate to other schools/settings in Kent.

Parents and children will need to work in partnership with Saplings to resolve issues.

**Responding to concerns regarding Indecent Images of Children**

Saplings will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.

Saplings will take action regarding Indecent Images of Children (IIOC) regardless of the use of Saplings equipment or personal equipment, both on and off the premises.

Saplings will take action to prevent access accidental access to of Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.

If Saplings is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

If Saplings are made aware of Indecent Images of Children (IIOC) then Saplings will:

* Act in accordance with Sapling's child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
* Immediately notify Saplings Designated Safeguard Lead.
* Store any devices involved securely.
* Immediately inform appropriate organisations e.g., the Internet Watch Foundation (IWF), Kent police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).

If Saplings are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, then Saplings will:

* Ensure that the Designated Safeguard Lead is informed.
* Ensure that the URLs (webpage 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.

If Saplings are made aware that indecent images of children have been found on Saplings electronic devices, then Saplings will:

* Ensure that the Designated Safeguard Lead is informed.
* Ensure that the URLs (webpage 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.
* Inform the police via 101 (999 if there is an immediate risk of harm) and children’s social services (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.

If Saplings are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:

* Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with Sapling's whistleblowing procedure.
* Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
* Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with Saplings managing allegations policy.
* Follow the appropriate Saplings policies regarding conduct.

**Online Safety (e-Safety) Contacts and References**

 **Kent Support and Guidance**

Kent County Councils Education Safeguards Team:

 [www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding](http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguardin)

**Kent Online Safety Support for Education Settings**

* Rebecca Avery, Education Safeguarding Adviser (Online Protection)
* Ashley Gorton, e-Safety Development Officer
* esafetyofficer@kent.gov.uk Tel: 03000 415797

**Kent Police:**

[www.kent.police.uk](http://www.kent.police.uk) or [www.kent.police.uk/internetsafety](http://www.kent.police.uk/internetsafety)

 In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

**Kent Public Service Network (KPSN):** [www.kpsn.net](http://www.kpsn.net)

**Kent Safeguarding Children Board (KSCB):** [www.kscb.org.uk](http://www.kscb.org.uk)

**Kent e–Safety Blog:** [www.kentesafety.wordpress.com](http://www.kentesafety.wordpress.com)

 **EiS** - ICT Support for Schools and Kent Schools Broadband Service Desk: [www.eiskent.co.uk](http://www.eiskent.co.uk)

**National Links and Resources Action Fraud:** [www.actionfraud.police.uk](http://www.actionfraud.police.uk)

**BBC WebWise:** [www.bbc.co.uk/webwise](http://www.bbc.co.uk/webwise)

**CEOP (Child Exploitation and Online Protection Centre):** [www.ceop.police.uk](http://www.ceop.police.uk)

**ChildLine:** [www.childline.org.uk](http://www.childline.org.uk)

**Childnet:** [www.childnet.com](http://www.childnet.com)

**Get Safe Online:** [www.getsafeonline.org](http://www.getsafeonline.org)

**Internet Matters:** [www.internetmatters.org](http://www.internetmatters.org)

**Internet Watch Foundation (IWF):** [www.iwf.org.uk](http://www.iwf.org.uk)

**Lucy Faithfull Foundation:** [www.lucyfaithfull.org](http://www.lucyfaithfull.org)

**Know the Net:** [www.knowthenet.org.uk](http://www.knowthenet.org.uk)

**Net Aware:** [www.net-aware.org.uk](http://www.net-aware.org.uk)

**NSPCC:** [www.nspcc.org.uk/onlinesafety](http://www.nspcc.org.uk/onlinesafety)

**Parent Port:** [www.parentport.org.uk](http://www.parentport.org.uk)

**Professional Online Safety Helpline:** [www.saferinternet.org.uk/about/helpline](http://www.saferinternet.org.uk/about/helpline)

**The Marie Collins Foundation:** <http://www.mariecollinsfoundation.org.uk/>

**Think U Know:** [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

**Virtual Global Taskforce:** [www.virtualglobaltaskforce.com](http://www.virtualglobaltaskforce.com)

**UK Safer Internet Centre:** [www.saferinternet.org.uk](http://www.saferinternet.org.uk)

**360 Safe Self-Review tool for schools:** <https://360safe.org.uk/>

**Online Compass (Self review tool for other settings):** <http://www.onlinecompass.org.uk/>