Online Safety Policy
Stepping Stones Short Stay School

Approved by:	Alison Dodd	Date: 22nd March 2022
Last reviewed on:	April 2020 – in line with COVID and remote learning May 2021	
Next review due by:	March 2023	

Contents

_____

1. Aims

Our school aims to:

> **Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors**

> **Deliver an effective approach to online 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**

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

> Teaching online safety in schools

> Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

> [Relationships and sex education – remove if not applicable, see section 4]

> Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if

necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board (Committee)

The Committee has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Committee will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The committee who oversees online safety is Amanda Sinker (Safeguarding)

All committee members will:

> Ensure that they have read and understand this policy

> Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL [and deputy/deputies] are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

> Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

> Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents

> Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

> Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

> Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)

> Liaising with other agencies and/or external services if necessary

> Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

At Stepping Stones, we purchase IT support from ED-IT, who undertakes the role of ICT manager in conjunction with the computing lead, Kirstie Hunter.

The ICT manager is responsible for:

> Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

> Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

> Conducting a full security check and monitoring the school's ICT systems on a monthly basis

> Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

> Ensuring that any online safety incidents are logged (see appendix 5) and breaches are reported to Alison Dodd (Head teacher)

3.5 All staff and volunteers

All staff, including contractors and agency staff, trainee teachers and volunteers are responsible for:

> Maintaining an understanding of this policy

> Undertaking training on Online Safety – regularly provided by The Key Safeguarding Centre and DSL's in school.

> Implementing this policy consistently and ensuring staff understand the procedures to implement when issues arise.

> Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)

> Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

> Ensuring that any incidents of cyber-bullying/ peer on peer abuse / online behaviour concerns are reported to DSL and the Head teacher in order for them to be addressed and dealt with accordingly. **(March 2022 introduction of Online / Concerns reporting form and Online concerns risk management plans)**

3.6 Parents

Parents are expected to:

> Notify a member of staff or the headteacher of any concerns or queries regarding this policy

> Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

> To monitor their child's use of IT / phones / devices / tablets etc at home.

> To report incidents to school without delay.

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

> Healthy relationships – Disrespect Nobody / Use of Brooke Education / NSPCC

> The School Updates its online safety webpage weekly with current updates to ensure parents are provided with up to date relevant information.

> https://www.steppingstones.lancs.sch.uk/keeping-your-child-safe-online/

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will

be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

Visitors will only be given access to the visitor network. Details can be received from the school office.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

In **Key Stage 1**, pupils will be taught to:

> Use technology safely and respectfully, keeping personal information private

> Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

> Use technology safely, respectfully and responsibly

> Recognise acceptable and unacceptable behaviour

> Identify a range of ways to report concerns about content and contact

*By the **end of primary school**, pupils will know:*

> *That people sometimes behave differently online, including by pretending to be someone they are not*

> *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*

> *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*

> *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*

> *How information and data is shared and used online*

> *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

The safe use of social media and the internet will also be covered in other subjects where relevant.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website, regular newsletters and through sharing materials from https://nationalonlinesafety.com/

This policy will also be shared with parents.

Online safety will also be covered during reporting to parents on curriculum areas.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Online Safety Concerns in Relation to the 4C's

All staff undertake training on Online Safety and are aware of the 4C's.

Content

Contact

Conduct

Commercial

Nature of Concerns				
	Commercial	Aggressive	Sexual	Values
Content (Child as recipient)	Adverts Span Sponsorship Sharing of personal info	Violent / hateful content Peer on peer abuse	Pornographic or unwelcome sexual content Harassment	Bias Racist Misleading info or advice
Contact (Child as participant)	Tracking Harvesting personal info	Being bullied, harassed or stalked Peer on peer abuse	Meeting strangers Being groomed Peer on peer abuse / harassment	Self-harm Unwelcome persuasions (sexual noises, inappropriate

				content)
Conduct	Illegal downloading Hacking Gambling Financial scams terrorism	Bullying or harassing another Peer on peer abuse	Creating and uploading inappropriate material Inappropriate conduct Taking and sharing nudes / semi nudes	Providing misleading information or advice

FURTHER DEFINITIONS WHEN DEALING WITH ONLINE BEHAVIOUR / CONCERNS

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Online Peer on Peer Abuse

Online peer-on-peer abuse is **any form of peer-on-peer abuse with a digital element**, for example, sexting, online abuse, coercion and exploitation, peer on peer grooming, threatening language delivered via online means, distribution of sexualised content and harassment.

Dealing with Peer on Peer Abuse

Staff with concerns of information shared from children or parents should report peer on peer abuse to the DSL immediately or on the day that information has come to fruition. The staff member should complete the online concern form / or disclosure form if the child is at immediate risk. E.g. to gather information for referrals to other agencies.

In line with the safeguarding policy and procedures the DSL's will make decisions based on the information shared and level of risk to child /ren.

Sexual Harassment (Information from Childnet.com)

In the [Project deSHAME report](#), online sexual harassment is defined as **unwanted sexual conduct** on any digital platform and it is recognised as a form of sexual violence.

Online sexual harassment encompasses a wide range of behaviours that use digital content (images, videos, posts, messages, pages) on a variety of different platforms (private or public).

It can make a person feel threatened, exploited, coerced, humiliated, upset, sexualised or discriminated against.

Dealing with Allegations of Sexual Harassment

In the event of information shared around unwanted sexual conduct or violence the school would take the appropriate actions in relation to safeguarding the child / ren from harm.

Staff would follow the school's policy for safeguarding, either completing an online safety concern or disclosure. They would immediately share information with the DSL team in order for the DSL's to take appropriate action and source appropriate support from other services and agencies, which may include the police.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

> Cause harm, and/or

> Disrupt teaching, and/or

> Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

> Delete that material, or

> Retain it as evidence (of a criminal offence or a breach of school discipline), and/or

> Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and the school's COVID-19 risk assessment.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Children at Stepping Stones should not be bringing any device into school. In some exceptional circumstance and when agreed with the Head teacher or Senior Leadership a mobile may be brought to school e.g. Y6 pupil who is home alone for short period of time and needs to have contact with parent. This would have a clear policy around. E.g. Child keeps the phone in their bag until arrival and the phone is stored in the office all day.

Any breaches of this rule can result in confiscation of the device pending parental collection.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Children should not bring their mobile devices to school. There is no need for the children to have their phones or alternative devices in school.

Any child who does bring their device should hand it to the class teacher. It will be stored in the school office for the day and returned to the taxi team to deliver home at the end of the day.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

> Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)

> Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device

> Making sure the device locks if left inactive for a period of time

> Not sharing the device among family or friends

> Installing anti-virus and anti-spyware software

> Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from Alison Dodd (Head teacher who will seek advice from ED -IT)

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use agreements. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. **(The Key Safeguarding Centre – Online Training)**

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL [and deputy/deputies] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by Alison Dodd, Head teacher. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

> Child protection and safeguarding policy
> Behaviour policy
> Staff disciplinary procedures
> Data protection policy and privacy notices
> Complaints procedure
> ICT and internet acceptable use policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
  - I click on a website by mistake
  - I receive messages from people I don't know
  - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If SLT have agreed for a personal mobile phone to be brought to school for safety purpose only

- I will not get it out of my bag on pupil transport.
- I will hand it to the school office on arrival.

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):	**Date:**

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS, TRAINEE TEACHERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/trainee teacher/visitor):	**Date:**

Appendix 4: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, trainee teachers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

- See Online Safety Reporting Form

- See Online Safety Risk Management Plan