School Improvement Liverpool

Online Safety Policy

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro

paul.bradshaw@si.liverpool.gov.uk 01.09.16

SUDLEY INFANT SCHOOL

ONLINE SAFETY POLICY

Vice Chair of governors

Mr S Kearney

Summer 2018 Review Summer 2019

Online Safety Policy

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

"Nothing is more important than promoting the welfare of children and protecting them from harm"

DFE, May 2016

(from the government's response to Alan Wood's, CBE – Review of the role and functions of Local Safeguarding Children Boards)

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation, sexual predation – technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify intervene and escalate any incident where appropriate.

DFE, May 2016

(from Annex C: Online Safety – Keeping Children Safe in Education)

Contents

- Digital images and video
- Storage, synchronizing & access

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Sudley Infant School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with children.

The main areas of risk for our school community can be summarised as follows:

<u>Content</u>

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

<u>Contact</u>

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

<u>Conduct</u>

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of Sudley Infant School community (including <u>ALL</u> staff, children, volunteers, parents or carers, visitors, community users) who have access to and are users of school IT systems, both in and out of Sudley Infant School.

Roles and responsibilities

Role	Key Responsibilities
Headteacher	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance. • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • To take overall responsibility for online safety provision. • To take overall responsibility for data management and information security ensuring school's provision follows best practice in information handling and is compliant with the eight principles of the Data Protection Act 1998 and GDPR from 25/5/2018. • To ensure the school uses appropriate IT systems and services including, a filtered Internet Service. • To be responsible for ensuring that ALL staff receive suitable training to carry out their safeguarding and online safety roles. • To be aware of procedures to be followed in the event of a serious online safety incident. • Ensure suitable 'risk assessments' are undertaken so the curriculum meets the needs of children, including the risk of children being radicalised. • To receive regular monitoring reports from the Designated Safeguarding Lead. • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures. • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety. • To ensure school that the school website includes relevant information and is compliant with the statutory requirements.
Designated Safeguarding Lead (online safety lead)	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents. • Promote an awareness and commitment to online safety throughout the school community. • Ensure that online safety education is embedded within the curriculum. • Liaise with school technical staff where appropriate. • To communicate regularly with SLT and the designated online safety Governors to discuss current issues, review incident logs and appropriate filtering/monitoring issues and change control logs. • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident. • To ensure that online safety incidents are logged as a

Role	Key Responsibilities
	safeguarding incident • Facilitate training and advice for ALL staff. • Oversee any child surveys/child feedback on online safety issues. • Liaise with the Local Authority and relevant agencies. • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
Governors/ Safeguarding governor	• To ensure that the school has in place policies and practices to keep the children and ALL staff safe online. • To approve the Online Safety Policy and review the effectiveness of the policy. • To support the school in encouraging parents or carers and the wider community to become engaged in online safety activities. • The role of the Safeguarding Governor will include: regular review with the Designated Safeguarding Lead about issues around online safety.
Computing subject leader	• To oversee the delivery of the online safety elements of the Computing Curriculum.
Admin officer/IT technician	• To report all online safety related issues that come to their attention, to the Designated Safeguarding Lead. • To manage the school's computer systems, ensuring - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus/malware/ransomware protection up to date). - access controls/encryption exist to protect personal and sensitive information held on school-owned devices. - the school's policy on appropriate web filtering and monitoring is applied and updated on a regular basis. • To keep up to date with the school online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as required. • To ensure school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Designated Safeguarding Lead/DSL/Headteacher • To ensure appropriate backup procedures and disaster recovery plans are in place, • To keep up-to-date documentation of the school's online security and technical procedures. • To ensure that the data they manage is accurate and up-to-date. • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements.

Role	Key Responsibilities
	• Ensure the school is registered with the Information Commissioner.
Teachers	• To embed online safety in the curriculum. • To supervise and guide children carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant). • To ensure that children are fully aware of research skills and are aware of legal issues such as copyright laws.
All staff, volunteers and contractors.	• To read, understand, sign and adhere to the school staff Acceptable Use Policy (AUP), and understand any updates - annually. The AUP is signed by new staff on induction. • To report any suspected misuse or problems to the Designated Safeguarding Lead. • To maintain an awareness of current online safety issues and guidance e.g. through relevant CPD. • To always model safe, responsible, respectful and professional behaviours in their own use of technology. • At the end of the period of employment returning any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager or computing subject leader on the last day to log in and allow a factory reset.
Children	• Read, understand, sign and adhere to the Child Online Safety Awareness Agreement. • To understand the importance of reporting abuse, misuse or access to inappropriate materials. • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To understand the importance of adopting safe, responsible and respectful behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school. • To contribute to any 'child voice'/surveys that gathers information of their online experiences.
Parents or carers	• To read, understand and promote the school's Child Online Safety Awareness Agreement with their child/ren. • To consult with the school if they have any concerns about how their child uses technology. • To support the school in promoting online safety and endorse the Social Media Guidelines for parents or carers which includes social media and use of photographic and video images
External groups including Parent groups	• Any external individual/organisation will sign an Acceptable Use Agreement prior to using technology or the Internet within school.

Role	Key Responsibilities
	• To support the school in promoting online safety. • To model safe, responsible, respectful and positive behaviours in their own use of technology.

Communication:

The policy will be communicated to staff/children/community in the following ways:

- Policy to be posted on the school website.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Guidance to be issued to whole school community, on entry to the school.

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.
- Staff and children are given information about infringements in use and possible sanctions.
- Designated Safeguarding Lead to act as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Designated Safeguarding Lead that day using the ‘online safety incident’ form.
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority’s Designated Officer).

Review and Monitoring

The Online Safety Policy is referenced within other school policies (e.g. Safeguarding and Child Protection Policy)

The Online Safety Policy is reviewed annually or when any significant changes occur with regard to the technologies in use within the school.

- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school Online Safety Policy will be disseminated to all members of staff and children.

2. Education and Curriculum

Child online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing Curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind children about their responsibilities through the Child Online Safety Awareness Agreement;

- ensures staff are aware of their responsibility to model safe, responsible, respectful and professional behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and children understand issues around plagiarism; and know that they must respect and acknowledge copyright/intellectual property rights;
- ensure children only use school-approved systems and publish within appropriately secure/age-appropriate environments.

Staff and governor training

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program;
- provides, as part of the induction process, all new staff (including those on university/college placement and work experience) with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.
- provides Safeguarding training for governors which includes online safety.

Parent awareness and training

This school:

- provides induction for parents which includes online safety;
- guidance and training for parents as well as providing online safety advice via the school's newsletter and website.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant guidelines or agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting safe, responsible and respectful online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices including cameras;

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable;
- know to take professional, reasonable precautions when working with children, previewing websites before use;
- using age-appropriate search engines where more open Internet searching is required with younger pupils e.g. Kiddle;

Parents or carers

- should know and understand what the school's rules of appropriate use for the whole school community in the use of social media are and what sanctions result from misuse.

Incident Management

In this school:

- all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively;
- support is actively sought from other agencies as needed (i.e. School Improvement Liverpool, UK Safer Internet Centre Helpline (0844 3814772/helpline@saferinternet.org.uk), CEOP, Prevent Officer, Merseyside Police, IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place if necessary and contributes to developments in policy and practice in online safety within the school;
- parents or carers are specifically informed of any online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or children receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Merseyside Police, Internet Watch Foundation and inform the Local Authority.

4. Managing IT and Communication System

Internet access, security (virus protection) and appropriate filtering and monitoring

This school:

- has filtered, secure broadband connectivity provided by Trustnet;
- uses Webscreen 2 which blocks sites that fall into categories (e.g. adult content, race hate, and gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- ensures network health through use of Sophos anti-virus software;
- uses approved systems to send 'protect-level' (sensitive personal) data over the Internet e.g. CTF pupil transfer/assessment data.
- works in partnership with School Improvement Liverpool/Liverpool City Council Connect2ICT to ensure any concerns are communicated so that systems remain robust and protect children.

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users – Trustnet;

- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Has additional local network monitoring software installed;
- Has daily back-up of school data (admin and curriculum);
- Ensures the Systems Administrator is up-to-date with their technical knowledge;
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- Storage of data within the school will conform to the EU and UK data protection requirements; Storage of data online will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's Online Safety Policy. Following this, they are set-up with Internet, email access and network access if necessary. Online access to service is through a unique username and password;
- Makes clear that no one should log on as another user and makes clear that children should never be allowed to log-on or use teacher and staff logins;
- Has set-up the network with a shared work area for staff. Staff and children are shown how to save work to this area and staff are shown how to access work from these areas;
- Requires all users to log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus/malware/ransomware protection;
- Makes clear that staff are responsible for ensuring that any computer/laptop/mobile device loaned to them by the school, is used only to support their professional responsibilities;
- Makes clear that staff accessing Local Authority systems do so in accordance with any corporate Liverpool City Council policies;
- Maintains equipment appropriately and reports any faults to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school approved systems;
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need;
- Has a disaster recovery system in place that includes a secure, remote off-site back up of data;
- Uses secure data transfer.
- Ensures that all child level data or personal data sent over the Internet is encrypted.
- Our wireless network has been secured to appropriate standards suitable for educational use;
- All IT and communications systems are installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password policy

- This school makes it clear that staff and children should always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords using a number and a combination of lower and upper case letters.

E-mail

This school

- Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account;
- Will contact the Police if one of our staff or children receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date.
- Uses a number of technologies to help protect users and systems in the school, including desktop anti-virus products, plus direct email filtering for viruses.
- Views comments which may be seen as intimidating, racist, sexist, homophobic or defamatory as cyber-bullying and will deal with them in accordance to school policy.

Children:

- Children are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Staff can only use school e-mail systems on the school system. Access in school to external personal e-mail accounts may be blocked
- Staff can only use the school e-mail systems for professional purposes.
- Sensitive or confidential data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data or file must be protected with security encryption.

School website

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school web site complies with statutory DFE requirements;
- Photographs published on the web do not have full names attached. We do not use children' names when saving images in the file names or in the tags when publishing to the school website;

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for children to use on a personal basis or to open up their own spaces to their children.

School staff will ensure that in private use:

- No reference should be made in social media to children, parents or carers or school staff;
- Never post images or videos of children.
- School staff should not be online friends with any children or parents or carers of children.
- If they receive a friend request from a child or parent/carer they should decline the invite and inform Leadership.
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- They regularly check security and privacy settings on personal social media profiles to minimise risk of loss of personal information.

Children:

- Are taught about safe, responsible, respectful and acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Are required to sign and follow our child Online Safety Awareness Agreement.

Parents:

- Are reminded about social networking risks and protocols through our Social Media Guidelines for parents, carers and governors as well as additional communications or materials when required.
- Are reminded that they should not upload photographs, videos or any other information about other people without their individual prior permission.
- Are encouraged to model safe, responsible and respectful use of social media for their children to emulate.
- As a school we believe that parents should be discouraged from using social media to criticise teaching staff and to make comments about our school and the community it serves. Any issues regarding a child's schooling should be addressed by speaking to the appropriate staff member. We are always happy to listen.

CCTV

- We have CCTV in some areas of the school as part of our site surveillance for staff and child safety. The use of CCTV is clearly signposted in the school and the images will only be used should it be necessary in the event of a Safeguarding incident.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).

- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are.
- We ensure staff know who to report any incidents where data protection may have been compromised to.
- All staff are DBS checked and records are held in a single central record.

Technical Solutions

- We use the TRUSTnet USO AutoUpdate, for creation of online user accounts for access to broadband services and the TRUSTnet content.
- All servers are in secure, lockable locations and managed by DBS-checked staff.
- Details of all school-owned hardware is recorded in a hardware inventory, including hardware on loan to named staff members.
- Details of all school-owned software is recorded in a software inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

6. Equipment and Digital Content

Personal Mobile Devices-general guidelines

- Personal mobile devices are considered to include mobile phones, tablets or other mobile devices.
- Mobile devices brought in to school are the responsibility of the device owner and are brought into school entirely at the staff member, child, parents, carers, governors or visitors own risk. The school accepts no responsibility for the loss, theft or damage of any personally-owned phone or hand held mobile devices brought into school.
- Mobile devices are not permitted to be used in certain areas within the school site, e.g. toilets. ‘Mobile-free’ signs to this effect are displayed.
- Visitors including volunteers/parent helpers should hand in any mobile devices to reception when they sign in. These will be stored securely until the person leaves.
- The recording, taking and sharing of images, video and audio on any personal mobile device is not allowed.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.

Staff use of personal mobile devices

- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting.
- Staff may be issued with a school phone where contact with children, parents or carers is required, for instance for off-site activities.

- Mobile Phones and personally-owned devices should be switched off or switched to ‘silent’ mode. Mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in exceptional or emergency circumstances.
- Staff members may use their phones during school break times when not in the company of children.
- If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Staff must not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of children and will only use work-provided equipment for this purpose.
- In an emergency where a staff member doesn’t have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes and then report the incident with the Headteacher / Designated Safeguarding Officer.
- Staff mobiles devices may be searched at any time as part of routine monitoring.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Children’s use of mobile devices

- No child should bring a mobile phone or personally-owned device into school. Any device brought into school will be confiscated and stored securely until it can be given to a parent.
- If a student breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents or carers as soon as possible.
- Children may be provided with school mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled.
- Children will be instructed in safe and appropriate use of mobile devices and tablets and will be made aware of safe use and consequences as part of the online safety elements of the Computing curriculum.

Digital images and video

In this school:

- We gain parent or carer permission for use of digital photographs or videos involving their child as part of the school agreement forms or when their daughter/son joins the school;
- We do not identify children in online photographic materials or include the full names of children in any published school produced video materials such as the school website;
- Staff sign the school’s Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of children;
- If specific child photos (not group photos) are used on the school website, in the prospectus or in other high profile publications the school will obtain individual parental permission for its long term, high profile use.

- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Children are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of the Computing scheme of work;
- Children are advised to be very careful about placing any personal photos on any 'social' online network space or when playing games online. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Children are taught that they should not post images or videos of others without their permission. We teach children about the risks associated with providing information via images that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Storage, Synchronizing and Access

- PIN access to the device must always be known by the network manager.
- If personal accounts are used for access to a school owned mobile or tablet device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.
- PIN access to the device must always be known by the network manager.
- Any information stored on a USB stick must be password protected.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

Appendices

Acceptable Use Agreement (Staff)
Online Safety Awareness Agreements (Children)
Social Media Guidelines (parents, carers and governors)
Online safety incident recording form