Online safety policy for

Early Years and Primary School settings

Hackney Learning Trust

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Date created | Written by | Review date | Reviewed by | Amendments | Authorised |
| 28/07/2015 | Jeremy Harris | September 2015 |  |  |  |
| 28/08/2015 | James Sykes | September 2015 | James Skyes | Jeremy Harris |  |
|  | Jeremy Harris | January 2016 | SLT | Jeremy Harris | SLT |

Table of Contents

[Online Safety Policy statement 3](#_Toc425928595)

[Scope 3](#_Toc425928596)

[Communication 3](#_Toc425928597)

[Handling complaints 4](#_Toc425928598)

[Review and Monitoring 4](#_Toc425928599)

[Named online safety lead – roles and responsibilities 4](#_Toc425928600)

[Definitions 5](#_Toc425928601)

[1. Use of ICT equipment 5](#_Toc425928602)

[2. Online safety and use of digital devices 6](#_Toc425928603)

[3. Equipment 6](#_Toc425928604)

[4. Internet access 6](#_Toc425928605)

[5. Email access 6](#_Toc425928606)

[6. Digital still and video images 7](#_Toc425928607)

[7. Data security 7](#_Toc425928608)

[8. Mobile phones 7](#_Toc425928609)

[9. Digital cameras 7](#_Toc425928610)

[10. Internet and social networking sites 8](#_Toc425928611)

[11. School Website 9](#_Toc425928612)

[12. Online bullying 9](#_Toc425928613)

[Conclusion 11](#_Toc425928614)

[Permission Form 11](#_Toc425928615)

Appendix

1. Roles and responsibilities
2. Staff Acceptable Use Policy
3. Parent/carer Acceptable Use Policy
4. School production example letter to parents
5. online safety incident form
6. Internet filtering change request form
7. Glossary of terms

# What is online safety?

Online safety is defined as being safe from risks to personal safety and wellbeing when using all fixed and mobile devices that allow access to the internet, as well as those that are used to communicate electronically.

It means ensuring that children and young people are protected from harm and supported to achieve the maximum benefit from new and developing technologies without risk to themselves or others. This includes personal computers, laptops, mobile phones and games consoles such as Xbox, Playstation and Wii.

The aim of promoting online safety is to protect young people from the adverse consequences of access or use of electronic media, including from bullying, inappropriate sexualised behaviour or exploitation

Safeguarding against these risks is not just an ICT responsibility, it is everyone’s responsibility, and needs to be considered as part of the overall arrangements in place that safeguard and promote the welfare of all members of the community, particularly those that are vulnerable.

The term 'safeguard' is defined for the purposes of this document in relation to online safety as the process of limiting risks to children when using technology through a combined approach to policies and procedures, infrastructure and education, underpinned by standards and inspection.

# Online safety policy statement

The aim of this policy is to ensure children, staff, Governors, students and volunteers use the school’s internet and Information and Communication Technology (ICT) equipment safely and appropriately, ensuring the best possible outcomes for our children.

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

Content:

* exposure to illegal, inappropriate or harmful material, including online pornography, ignoring age ratings in games (exposure to violence and inappropriate language);
* lifestyle websites, for example pro-anorexia/self-harm/suicide sites;
* hate sites;
* content validation: how to check authenticity and accuracy of online content.

Contact:

* being subjected to harmful online interaction with other users;
* grooming;
* child sexual exploitation
* cyber-bullying in all forms;
* extremism and radicalisation
* identity theft and sharing passwords.

Conduct:

* personal online behaviour that increases the likelihood of, or causes, harm;
* privacy issues, including disclosure of personal information;
* digital footprint and online reputation;
* health and well-being (amount of time spent online (socialising, watching video or gaming));
* sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images);
* copyright (no thought or consideration for intellectual property and ownership – such as music and film).

## Scope

This policy applies to all members of [name of setting] community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of setting ICT systems, both in and out of [name of school].

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

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

This policy has been created in line with the statutory guidance document **Keeping Children Safe in Education, 2015.**

See appendix for description of roles and responsibilities.

## Communication

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

* Policy to be posted on the school website/ staffroom/ classrooms/play areas;
* Policy to be part of school induction pack for new staff;
* School will provide a ‘Safe Internet’ page for parents on the school website. Information will include internet safety advice, home web filtering tips and links to recommended online safety websites; and guidance on the amount of time children may spend on a computer, smartphone, tablet or games console;
* Acceptable Use agreements discussed with pupils and their families at the start of each year;
* Acceptable Use agreements to be issued to whole school community, usually on entry to the setting;
* Acceptable Use agreements to be held in pupil and personnel files;
* Children and teachers will be provided with training in the area of online safety.

## Handling complaints

* The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of internet access;
* Staff and pupils are given information about infringements in use and possible sanctions; Sanctions available include:
	+ interview/counselling by Online Safety Lead / Head teacher;
	+ informing parents or carers;
	+ removal of internet or computer access for a period;
	+ referral to Local Authority, Children’s Social Care and/or police.
* Our Online safety Lead acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head teacher;
* Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy; Complaints and/or allegations related to child protection are dealt with in accordance with the school and Local Authority child protection procedures:
* All complaints will be dealt with in accordance with our Complaints Policy.

## Review and Monitoring

The online safety policy is referenced from within other school policies: ICT and Computing policy, Child Safeguarding and Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education and for Citizenship policies [check which of these policies refer to online safety/e-safety and include as appropriate]

* The school has an online safety Lead who will be responsible for document ownership, review and updates;
* The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school;
* The online safety policy has been written by the school online safety Coordinator and is current and appropriate for its intended audience and purpose;
* There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders such as the PTA [check]. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff;
* The online safety policy will be reviewed biennially.

## Named online safety lead – roles and responsibilities

A named online safety lead is crucial to developing and maintaining an online safety culture within the early years setting. The named person will usually be the designated member of staff for safeguarding or the member of staff able to cover for them in their absence.

The responsibilities of this role are to:

1. Develop an online safety culture at [name of school or setting];
2. Be the named point of contact on all online safety issues;
3. Ensure online safety is included as part of the induction procedures and an Acceptable Use Policy is signed and dated by staff and volunteers;
4. Monitor online safety, such as:
	1. ensuring the infrastructure of technology provides a safe and secure environment for children, for example by ensuring web address filters and other software security are in place;
	2. maintaining an online safety incident log to record concerns and incidents;
	3. reporting on online safety issues to the management team and directors/governors/ management committee;
5. Ensure that all staff, volunteers and directors/governors/management committee members know what to do if they are concerned about an online safety issue;
6. Keep abreast of developing online safety issues via:
	1. http://www.saferinternet.org.uk/
7. Ensure that online safety is embedded within continuing professional development (CPD) for staff and volunteers, and co-ordinate training as appropriate;
8. Ensure that online safety is embedded across all activities as appropriate;
9. Ensure that online safety is promoted to parents/carers, children and others in the setting, the home and the community;
10. Review and update online safety policies and procedures on a regular basis and after an incident.

## Definitions

What do we mean by ‘online’?

When we refer to being online we include being connected to the internet or communicating through a wide range of devices or technologies, such as computers, laptops, mobile phones, tablet computers, hand-held devices and games consoles

Setting

Includes any Early Years and childcare provision for children from birth to five, and any out of school provision for children and young people, such as playgroups, pre-schools, childminders, nurseries, Children’s Centres and after-school clubs.

Other definitions

The term parent/carer refers to any individual who has a parental responsibility for a child or has care of a child.

# Use of ICT equipment

**Children should never be allowed to use the internet in the setting without adult supervision**

Staff who use the centre’s ICT and communications systems:

1. Must sign an Acceptable Use Policy;
2. Must use the systems responsibly and keep them safe;
3. Must maintain safe professional boundaries with parents. This includes not giving their personal email address to school users or befriending school users on social network sites such as Facebook;
4. Must treat as confidential any passwords provided to allow access to all ICT equipment;
5. Must ensure integrity of passwords. Network user account passwords should be strong (mixture of letters, number and characters) and be changed periodically, e.g. monthly. If a password is compromised, it must be changed as soon as possible and no longer than within 24 hours;
6. Must not install software on the school’s equipment, including freeware and shareware;
7. No personal devices (e.g. USB memory sticks) should be used to upload or download material onto the school network or website, or any ICT device;
	1. The school provides encrypted USB memory sticks for staff to use [verify];
8. Use of cloud storage systems (e.g. Dropbox or iCloud) must be approved by either the online safety lead, Deputy Headteacher or Headteacher;
9. Must comply with any ICT security procedures governing the use of systems in the school, including anti-virus measures;
10. Must report known breaches of this policy, including any inappropriate images, messages or other material which may be discovered on the school’s ICT systems;
11. Must ensure that the systems are used in compliance with this online safety policy;
12. Staff, volunteers and children will be provided with training in the area of online safety.

# Online safety and use of digital devices

At all times, children, staff, Governors, Parents, students and volunteers will treat others with respect and will not undertake any actions that may bring the school into disrepute.

Mobile phones, tablets and other digital devices can present a number of problems when not used appropriately:

1. Mobile/smartphones and personal devices can allow wireless and 3G/4G internet access via alternative ISPs, and therefore bypass the school’s central security settings and filtering;
2. Mobile/smartphones with integrated cameras could lead to child protection, bullying, and data protection issues with regard to inappropriate capture, use or distribution of images of children or staff.

# Equipment

All computer equipment is installed professionally and meets current health and safety standards. Equipment is maintained to ensure health and safety standards are followed.

# Internet access

School’s Internet Service Provider (ISP) is London Grid for Learning (LGfL). LGfL is a Regional Broadband Consortium, and provides services to the majority of schools across the 33 boroughs of London via its partnership with Virgin Media Business. LGfL provides internet filtering based on the Internet Watch Foundation (www.iwf.org.uk) model via its Websweeper 2.0 software [check].

# Email access

School uses [name of email filtering system] to detect and block viruses, spam, phishing, Trojan, and other malicious message types, and inappropriate language [check with Hackney Learning Trust ICT Services].

We:

1. use standard school-issued email addresses;
2. staff and volunteers will use only a school-issued email account for their professional use;
3. Staff, volunteers, Governors and all those connected professionally with school will not send material that is illegal, obscene, upsetting or defamatory, or that is intended to annoy or intimidate another person. Should such content be received, it must not be forwarded to anyone, and must be reported to the online safety co-ordinator, who will take appropriate action;
4. know that spam, phishing, Trojan and virus attachments are a danger to the school’s systems.

# Digital still and video images

1. We gain written parental/carer permission for use of digital photographs or video involving their child as part of the agreement form when their child joins [name of setting here]
2. Digital images/videos of children are stored in a hidden “Pupil images” folder on the school network, which only named individuals have access to [check]. All Images are deleted at the end of the academic year.

# Data security

1. Personal data is stored securely. Access to personal data is strictly controlled by the Designated Safeguarding Lead;
2. Data is secured against loss through systems failure, theft and damage [how? Check with HLT IT Services or the school’s/setting’s IT provider];
3. If personal or sensitive data, defined as being covered by the Data Protection Act, needs to be transmitted, it is done so securely. Data is password protected, and the password will be transmitted separately;
4. The use of electronic equipment off-site must be formally approved, in writing, by the user’s line manager;
5. The school/setting is registered with the Information Commissioner’s Office;
6. An incident management log is maintained by the online safety/data security lead;
7. Data security incidents must be reported through the appropriate internal management channels as quickly as possible after the incident or awareness of the incident;
8. Serious incidents of data breaches should be reported to the Information Commissioner’s Office;
9. All electronic equipment that is to be reused or disposed of will have all of its data and software erased/destroyed, in accordance with the HSE’s WEEE directive;
10. Data security is reviewed annually, and staff updated annually.

# Mobile phones

1. Staff should not have personal mobile phones with them when they are working with children at the setting. These conditions also apply to students and volunteers;
2. Staff mobile phones must be kept in staff lockers [needs verifying] and used only when staff are on break time in the staff room or outside the setting;
3. Staff are not permitted to use their own personal phones or devices for contacting children and their families within or outside of the setting in a professional capacity;
	1. The telephone number of the centre should be used by staff in all communication with families, and for emergency contact;
4. Keeping mobile phones in rooms while working with children constitutes a staff disciplinary matter, and may lead to staff and volunteers’ placement being terminated;
5. Setting mobile phones should be used for off-site activities, home visits and outings. Staff are not permitted to use their mobile phones whilst out of the setting on an outing [needs verifying];
6. Parents, carers and visitors are requested not to use their mobile phones while on the school premises. School staff will remind parents, carers and all visitors of the policy by reminding them to switch off their phones when they enter the setting or asking them to leave the rooms to make or receive calls in the reception area/foyer when necessary.

# Digital cameras

1. Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils, and will only use work-provided equipment for this purpose;
2. We gain written parental/carer permission for use of digital photographs or video involving their child as part of the agreement form when their child joins;
3. Children can only be photographed if permission of parents/carers is given;
4. Personal cameras are not allowed in the setting and should not be used on off-site activities, home visits and outings;
5. The setting holds a number of digital cameras for staff and, where appropriate, for parents, carers, students and volunteers to take photographs of children for display, observations or profile books;
6. Use of video equipment can be a legitimate learning/training aid. Children and parents/ carers should be made aware that this is part of the learning/training;
7. Students, volunteers and visitors are not permitted to take photographs or recordings of the children without permission from the Head of setting or deputy head and with prior written consent from the parents/carers;
8. No one is permitted to photograph or record images in the toilet and changing areas;
9. Photographers will be required to have clear formal identification which must be worn at all times, for example at an open day or event;
10. Children’s images will not be used for promotional or press releases unless parents/carers have given prior written consent.

#  Internet and social networking sites

1. Internet access at school will always be overseen by a member of staff;
2. Access to websites for children are limited to those agreed by the school only;
3. School staff and volunteers will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials on school equipment;
4. School staff will report accidental accessing of inappropriate materials in accordance with school procedures;
5. Staff, volunteers and children will use the Internet for educational purposes only;
6. The school will NEVER knowingly disclose or publicise personal information relating to children on any social media platform without explicit consent. Personal information means data which relate to a living individual who can be identified from those data; *(needs tidying up)*
7. Downloading materials or images not relevant to teaching and learning is in direct breach of school policy;
8. School staff will be aware that all internet activity, including distributing or receiving information, school-related or personal, will be monitored for unusual activity, security and/or network management reasons;
9. Staff are instructed not to create or manage social network spaces for pupil use on a personal basis, or to open up their own personal spaces to their pupils or the pupils’ families;
10. Staff must not search for, visit or monitor social networking presences of pupils or families.
	1. If a staff member does happen to find such a social network site or presence, they must not enter them. This is uninvited intrusion into a family’s life, and you and your employer are liable to investigation if you act outside these guidelines. If you have safeguarding/child protection concerns about a child’s/young person’s behaviour on-line, or if you think a social media platform could provide critical information, for example, if a child is missing or is at risk of harm, the police and children’s social care must be contacted. If warranted, the only agency that can access these sites is the police.
11. School staff will ensure that in private use:
12. No reference should be made in social media to pupils, parents/carers or school staff;
13. They do not engage in online discussion on personal matters relating to members of the setting community or the setting’s activities in any negative context, and/or actions that may bring an individual, profession or setting’s reputation into disrepute
14. Personal opinions should not be attributed to the school or Local Authority;
15. Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information [are they? Remove if not]

#  School website

1. Children’s learning will be published on the school website in-accordance with agreement from parents/carers;
2. The website will be edited only by an agreed number of staff which currently includes: Teacher responsible for ICT, DHT, HT, Bursar, Clerical Assistant, Head of Centre and the Learning Support Co-ordinator. All information placed on the website must adhere to the ethos and values of the school’s online safety Policy (note: add/delete as appropriate);
3. Personal pupil information including home address and contact details will be omitted from school web pages;
4. The school website will not publish the surnames of any pupils;
5. The school will ensure that the image files are appropriately named – and do not use pupils’ names in image files if published on the web;
6. School will ensure the web hosting company has a published security protocol.

#  Online bullying

Early years children are unlikely to be victims or perpetrators of online bullying, but their parents/ carers and/or older siblings may be, as may staff and volunteers at the nursery/children’s centre.

Bullying is defined in guidance issued by the Department of Education as: ‘behaviour by an individual or group, repeated over time, that intentionally hurts another individual or group either physically or emotionally’1

**What is online bullying?**

Online bullying is the use of technology, for example mobile phone, email, social networking sites, chat rooms and instant messaging services, to deliberately upset someone else

* It can be used to carry out different types of bullying, as an extension of face-to-face bullying;
	+ It can also go further as it can invade home/personal space and can involve a greater number of people;
* It is an anonymous method by which bullies can torment their victims at any time of day or night;
* It can draw bystanders into being accessories;
* It includes: threats and intimidation; harassment or ‘cyber-stalking’; vilification/defamation; exclusion or peer rejection; impersonation; unauthorised publication of private information or images (i.e. possible breach of copyright); and manipulation;
* It includes sexting - sending explicit images electronically. These images can be subsequently widely distributed;
* It also includes trolling; the practice of posting upsetting, provocative, offensive or off-topic messages in an online community. Trolling comments are posted with the deliberate intent of provoking readers into an emotional response, or of otherwise disrupting normal on-topic discussion.

**Impact on the victim**

The victim may receive email, chat, text messages or posts on social networking sites that make them feel embarrassed, upset, depressed or afraid. This can damage their self-esteem and pose a threat to their psychological wellbeing. Online bullying can pose a serious threat to their physical and emotional safety.

**Responding to online bullying**

Most cases of online bullying can be dealt with through anti-bullying policies and procedures.

For examples of responding to bullying please refer to CHSCB’s sample safeguarding/child protection policies:

<http://www.chscb.org.uk/content/41/>

In all cases of online bullying make sure that you preserve the evidence.

Some features of online bullying differ from other forms of bullying and may prompt a particular response. For example:

* Consider the bystanders; they can amount to hundreds of people;
* Change the victim’s mobile phone number;
* Report the bullying to the site where it was posted;
* Try to get content removed from the web;
* In some cases, the victim may be able to block the perpetrator from their sites and services;
* Ask the person bullying to delete the offending content and say who they have sent it on to;
* Contact the police in cases of actual/suspected illegal content.

What to do if you have concerns about a child

Staff and volunteers should follow the same procedures as for all other safeguarding issues and follow guidelines set out in Keeping Children Safe in Education 2015 statutory guidance.

How we manage allegations against a member of staff

Staff and volunteers should follow the same procedures as for all other safeguarding issues and follow guidelines set out in Keeping Children Safe in Education 2015 statutory guidance.

# Conclusion

The school recognises that the use of the technology, including access to the internet and ICT devices, can substantially and positively impact the quality of teaching and learning of our children and staff. This policy aims to ensure that such use is done safely and appropriately.

## Permission Form

Please review the attached school’s Online Safety Policy, sign and return this permission form to the Head teacher

School Name:

Child’s Name

Date:

**Parent/Guardian**

As the parent or legal guardian of the above pupil, I confirm I have read the Online safety policy and grant permission for my son or daughter or the child in my care to have full access to technology at [name of setting], including access to the internet. I understand that internet access is intended for educational purposes only. I also understand that every reasonable precaution has been taken by the school to provide for online safety but the school cannot be held responsible if pupils access unsuitable websites.

**I accept the above paragraph I do not accept the above paragraph**

(Please tick as appropriate)

In relation to the school website, I accept that, if the school considers it appropriate, my child’s schoolwork may be chosen for inclusion on the website. I understand and accept the terms of the online safety Policy relating to publishing children’s work on the school website.

**I accept the above paragraph I do not accept the above paragraph**

(Please tick as appropriate)

Signature: Date:

Address:

Telephone:

Reference:

1, Preventing and tackling bullying, Advice for Headteachers, staff and governing bodies, October 2014, Department for Education