Early Years online safety policy

for settings and Childminders

Hackney Learning Trust

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Date created | Written by | Review date | Reviewed by | Amendments | Authorised |
| 28/07/2015 | Jeremy Harris | September 2015 |  |  |  |
| 14/08/2015 |  | September 2015 | Nikki Baird | NB/JH |  |
| 26/02/2016 |  | February 2016 | Jeremy Harris | JH |  |

Table of Contents

[What is e-Safety? 3](#_Toc430595451)

[e-Safety policy statement 3](#_Toc430595452)

[Who this policy applies to 3](#_Toc430595453)

[Good practice 4](#_Toc430595454)

[How to find out about this policy 4](#_Toc430595455)

[Reporting concerns 4](#_Toc430595456)

[Review and Monitoring 4](#_Toc430595457)

[Named Online Safety lead – roles and responsibilities 4](#_Toc430595458)

[1. Use of technology 4](#_Toc430595459)

[1. E-Safety and use of digital devices 5](#_Toc430595460)

[2. Email access 5](#_Toc430595461)

[3. Photographs and video 5](#_Toc430595462)

[4. Data security 5](#_Toc430595463)

[5. Mobile phones 5](#_Toc430595464)

[7. Use of images of children 6](#_Toc430595465)

[8. Internet access and social networking sites 6](#_Toc430595466)

[9. Setting website 6](#_Toc430595467)

[10. Online bullying 6](#_Toc430595468)

[Conclusion 7](#_Toc430595469)

[**Parent/carer** 8](#_Toc430595470)

Appendix

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

# What is e-Safety?

e-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 e-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 e-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.

# e-Safety policy statement

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

The main areas of online safety risk can be described as follows:

Content:

* exposure to inappropriate content, 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:

* grooming;
* child sexual exploitation;
* cyber-bullying in all forms;
* extremism and radicalisation;
* identity theft and sharing passwords.

Conduct:

* 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.

## Who this policy applies to

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

## Good practice

## How to find out about this policy

You can find out about this policy in the following ways:

* Policy displayed in the setting
* Policy on the website;
* Policy to be part of induction for all staff and volunteers;
* Acceptable Use agreements to be signed by all staff/management and volunteers;
* Acceptable Use agreements to be issued to anyone using the settings ICT, including parents;
* The settings management is responsible for online safety, and answer any questions you may have.

## Reporting concerns

* The setting will take all reasonable precautions to ensure e-safety;
* All concerns must be reported to the settings manager;
* Staff/management, volunteers and parents will be given clear guidance regarding acceptable behaviour and anything that might cause concern;
* Concerns related to child protection are dealt with in accordance with the setting’s safeguarding and child protection procedures.

## Review and Monitoring

We will monitored and review this policy regularly, and at least annually.

## Named Online Safety lead – roles and responsibilities

A named e-safety lead is helpful in developing and maintaining an e-safety culture within the setting. This will usually be the setting’s manager.

The responsibilities of this role are to:

1. Develop a culture of online safety at [name of setting];
2. Be the named point of contact on all e-safety issues;
3. Ensure e-safety is included as part of the induction procedures and an Acceptable Use Policy is signed and dated by staff and volunteers;
4. Monitor e-safety, such as:
   1. ensuring filters and other security is in place;
   2. maintaining an e-safety incident log to record concerns and incidents;
5. Ensure that all staff, volunteers and management know what to do if they are concerned about an online safety issue;
6. Keep up-to-date with e-safety issues;
7. Ensure that e-safety is embedded across all activities as appropriate;
8. Ensure that e-safety is promoted to parents/carers, children and others in the setting, the home and the community;
9. Review and update e-safety policies and procedures.

# Use of technology

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

Staff/volunteers and management who use the setting’s computer and communications systems:

1. Must use the systems responsibly and keep them safe;
2. Must maintain safe professional boundaries with parents, for example communicating with parents via email and social networking sites;
3. Must sign an Acceptable Use Policy.

# E-Safety and use of digital devices

All staff/volunteers, management, parents and children will treat others with respect and will not undertake any actions that may bring the setting into disrepute.

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

1. Mobile/smartphones and personal devices can allow unfiltered internet access, and therefore bypass the setting’s security settings and filtering;
2. Mobile/smartphones/personal devices with integrated cameras could lead to child protection issues, bullying, and data protection issues, e.g. use or distribution of images of children or staff.

# Email access

Staff/volunteers and management will:

1. use only a setting-issued email account for their professional use;
2. not send material that is illegal, obscene, upsetting or defamatory, or that is intended to annoy or intimidate another person.

# Photographs and video

1. We gain written parental/carer permission for use of digital photographs or video involving their child/children as part of the agreement form when their child joins the setting
2. Digital images/videos of children are stored appropriately.

# Data security

1. Personal data is stored securely and access to personal data is strictly controlled by the Designated Safeguarding Lead (DSL)
2. If sensitive data, defined as being covered by the Data Protection Act, needs to be transferred, it is done so securely;
3. Data security incidents must be reported to, and dealt with by, the setting’s management;
4. If necessary, the setting is registered with the Information Commissioner’s Office;
5. All electronic equipment that is to be reused or disposed of will have all of its data and software erased/destroyed, and will be certified as such;
6. Data security is reviewed annually, and staff updated annually.

# Mobile phones

1. Staff must be aware of the setting’s mobile phone use policy;
2. Staff should not have personal mobile phones with them when they are working with children at the setting. This also applies to students and volunteers;
3. Parents, carers and visitors are requested not to use their mobile phones while on the setting’s premises
4. Using mobile phones in rooms while working with children may constitute a staff disciplinary matter;
5. 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 make or receive calls in the reception area/foyer when necessary.

# Use of images of children

1. Staff must be aware of the setting’s photograph policy;
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 is given by parents/carers;
4. 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 setting’s learning/training approach;
5. Students, volunteers and visitors are not permitted to take photographs or recordings of the children without permission from the setting’s manager and with consent from the parents/carers;
6. No one is permitted to photograph or record images in the toilet and changing areas;
7. External photographers will be required to wear clear identification at all times, e.g. at an event;
8. Children’s images will not be used for promotional or press releases unless parents/carers have given prior written consent.

# Internet access and social networking sites

1. The setting must ensure it has age-appropriate internet filtering in place.;
2. Internet access for children will always be overseen by a member of staff;
3. Access to websites for children are limited to those agreed by the setting;
4. Staff will be aware of online safety guidelines and abide by the setting’s Acceptable Use Policy
5. Staff must be professional at all times when using the internet at the setting

# Setting website

1. A setting website must not contain any personal information relating to children and parents, and must respect privacy of all staff/volunteers and management;
2. All information placed on the website, and links leading from it, must adhere to the ethos and values of the setting;

# 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 setting.

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’

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

**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 the setting’s anti-bullying and behaviour policies and procedures.

**Reporting concerns**

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

This setting recognises that the use of the technology, including access to the internet and ICT devices, can substantially and positively impact the educational development of our children and staff. This policy aims to ensure that such use is done safely and appropriately.

I confirm I have read and agree with the setting’s online safety policy:

Setting name:

**Staff/volunteer/management/student**

Name:

Role:

Signature:

Date:

**Parent/carer**

Name/s:

Signature/s: Date:

Address:

Telephone: