Effra Early Years Centre

Date agreed September 2016	Review Cycle 3 years	Due for review September 2019
Signed		

E- Safety Policy

Effra Early Years Centre is committed to safeguarding and promoting the welfare of children and expects all staff and volunteers to share this commitment.

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at Effra Early Years Centre we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

E-safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and ICT environment for Effra Early Years Centre.

Our e-safety Policy has been written by the school, following government guidance. It has been agreed and approved by governors.

- The school's e-safety coordinator is Angela Couchman
- The e-Safety Governor is Catherine Bewley

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. The role of the E-Safety Governor will include:

As part of our commitment to safeguarding, the governor with responsibility for safeguarding will monitor e-safety and will discuss any issues with the e-safety co-ordinator as part of their termly safeguarding monitoring.

Headteachers and Senior Leaders:

- The Headteachers are responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the e-Safety Co-ordinator.
- The Headteachers/Senior Leaders are responsible for ensuring that the e-safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteachers/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteachers and senior leaders should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The E-Safety Co-ordinator:

- Takes day-to day-responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Liaises with school ICT technical staff.
- Receives reports of any e-safety incidents and creates a log of incidents to inform future e-safety developments.

Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the Early Years Foundation Stage curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with access to a range of technology as part of their daily curriculum access:

- The school Internet access will be designed expressly for the children to use including appropriate content filtering via LGFL.
- Children will be supported to use technology and to consider why some websites may be ‘blocked’
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion,
language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet

the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society.

Authorised Internet Access

By explicitly authorising use of the school's Internet access children, staff, governors and parents are provided with information relating to e-safety and agree to its use:

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that children will be provided with closely supervised Internet access.
- Only authorised equipment, software and Internet access can be used within the school.

Internet

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning and sharing are some of the legitimate and beneficial uses. It can offer us exciting learning opportunities, however, there are inappropriate and undesirable elements that must be managed:

- Any inappropriate sites that are not filtered by LGFL will be reported to the e-Safety Safety Co-ordinator.
- Staff will be vigilant if children are accessing the internet on either of our two class based computers.
- The school will ensure that the use of Internet derived materials by staff and children complies with copyright law.

E-mail

- E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:
- Use of email by staff should be for work purposes if accessing through computers across the Effra site.
- E-mail sent to external organisations by staff should be written carefully
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Staff should never share passwords. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be ‘locked’).

Social Networking

- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered from a centre computer by LGFL.
- Our pupils are too young to have any access to social media, but we understand their parents and carers may have social media accounts.
- Parents, carers and staff will be advised of the dangers of discussing any aspects of the centre on social networking sites. The governors will consider taking legal action, where appropriate, to protect children and staff against cyber bullying and defamatory comments.

Reporting

All breaches of the e-safety policy need to be recorded in the E-Safety reporting book that is kept in the general office. The details of the user, date and incident should be reported.

Incidents which may lead to child protection issues need to be passed on to one of the Designated Persons for child protection immediately – it is their responsibility to decide on appropriate action not the staff member.

Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse then it should be handled according to the DFE document titled ‘Dealing with allegations of abuse against teachers and other staff’. If necessary the local authority’s LADO should be informed.

Evidence of incidents must be preserved and retained.

Mobile Phones and iPads

Almost all mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Staff should always use the school phone to contact parents, never personal mobiles
- Staff including students and visitors and parents are not permitted to access or use their mobile phones within the centre. All staff, visitors and volunteers should ensure that their phones are turned off and stored safely away during the day.

- Effra childrens' centre at Brockwell is included in this policy. No visitors to the site are permitted to have mobile phones visible while at the Brockwell site. A centre camera will be made available for child minders or crèche workers to photograph any evidence of learning. Photos will then be printed out and made available the following week.
- Staff may use their mobile phones in the staffroom or the school office.
- The staff may use centre owned tablets or iPads to record the children's learning. We have purchased a tool through 2Simple- 2 Build a profile to enable us to do this. All iPads are password protected and tracked through SBS. All information is stored in a secure cloud location and has additional password protection to access the photos and information. It is subject to Data Protection Act.
- During events at the centre parents and carers are no permitted to use mobile phones or other photographic equipment to photograph children.
- Lone worker such as outreach staff have work mobiles for business use only.

On trips staff mobiles are used for emergency only

Digital/Video Cameras/Photographs

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

Staff should always use a school camera to capture images and should not use their personal devices.

Photos taken by the centre are subject to the Data Protection act.

Published Content and the School Website

The school website is a valuable source of information for parents, carers and potential families.

- Contact details on the Website will be the school address, e-mail and telephone number.
- Staff personal information will not be published.
- The headteacher or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs and videos that include children will only be used with permission from families.
- Pupils' full names will not be used in association with photographs.
- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the IT management contracted by the centre.
- E-safety will be discussed with our ICT support and those arrangements incorporated in to our agreement with them.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act

Assessing Risk

The school will take all reasonable precautions to prevent access to inappropriate material, and will report any material we deem inappropriate to the e-safety co-ordinator for logging and to LGFL.

.

Handling E-Safety Complaints

- Any complaint about staff misuse must be referred to the Headteacher or member of the senior leadership team..
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.