**Ilminster Avenue Specialist Nursery School E-Safety Policy**

**Date Agreed: December 17 Review Date: December 18**

**Signed by: Signature:**

**Headteacher to decide**

**Role of Signatory:**

**1. Rationale**

Ilminster Avenue Specialist Nursery School (IASNS) understands its responsibility to educate staff, children and families in e-Safety issues. This entails teaching appropriate behaviours and critical thinking to enable users to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. This e-Safety policy therefore aims to clarify the responsibilities of management and staff and services users when using cameras, mobile phones, computers and games consoles within the setting, to safeguard children’s welfare in relation to the above areas and minimize the risk of harm and to fulfil legal duties in relation to personal data and other areas, e.g.: Data Protection Act 1998.

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, educational settings need to build in the use of these technologies in order to arm our children with the skills to access life-long learning and employment. Information and Communications Technology (ICT) covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

• Websites

• Learning Platforms and Virtual Learning Environments

• Email and Instant Messaging

• Chat Rooms and Social Networking

• Blogs and Wikis

• Podcasting

• Video Broadcasting

• Music Downloading

• Gaming

• Mobile/Smart phones with text, video and/or web functionality

• Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

This policy is inclusive of both fixed and mobile internet; technologies provided by the centre; (such as PCs, laptops, webcams, whiteboards, digital video equipment, etc.); and technologies owned by families and staff, but brought onto the Setting’s premises (such as laptops, mobile phones, camera phones and portable media players, etc.).

This policy works in conjunction with the following policies: Behaviour, Code of Conduct, Complaints, Equalities, Health and Safety and Safeguarding and Child Protection.

**2.** **Responsibilities**

**2.1 Governors**

Governors are responsible for the approval of the policy and for reviewing the effectiveness of the Policy. Governors should ensure that a named e-Safety Governor is appointed.

The role of the E-Safety Governors will include:

* Regular meetings with the E-Safety Leader
* Regular monitoring of E-Safety incident logs
* Reporting to relevant Governors’ meetings

The E-Safety Governor for the Setting is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**2.2 Headteacher and Senior Leaders**

The Headteacher is responsible for ensuring the overall safety (including E-Safety) of members of the setting’s community (though the day to day responsibility of E-Safety will be delegated to the E-Safety Leader).

The Headteacher/Senior Leaders are responsible for:

* appointing the e-Safety Leader for the Setting: Morgan Hardy
* ensuring that the E-Safety Leader and other relevant staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues, as relevant
* ensuring that there is a system in place to allow for monitoring and support of those in the setting 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
* following procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff

**2.3 E-Safety Leader**

The Setting will appoint an E-Safety Leader with responsibility for the e-Safety policy and procedures. Their duties will include:

* reviewing the setting’s E-Safety Policy/documents.
* ensuring that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
* providing training and advice for staff as appropriate.
* liaising with the Local Authority
* liaising with the setting’s ICT technical staff
* receiving reports of E-Safety incidents
* creating, maintaining and reviewing a log of incidents to inform future E-Safety developments.
* meeting regularly with E-Safety Governor to discuss current issues, review incident logs.
* attending relevant meetings and delivering e-Safety reports as required.

**2.4 All Staff**

Staff duties include:

* receiving regular information and training on e-Safety issues through the coordinator at staff meetings
* being made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the Setting’s community
* signing the Acceptable Use Agreement as part of their Induction
* incorporating e-Safety activities and awareness within their sessions

**2.5 Parents/carers**

Parents/carers will:

* sign the Acceptable Use of IT Agreement if they use the internet in the Setting.
* decide as to whether they consent to images of their child being taken/used on the Setting’s website
* be made aware of useful information and links to sites like Thinkuknow, Childline, CEOP and the CBBC Web Stay safe page, and other e-Safety information through newsletters, the website, and the prospectus sent out by the Setting to help keep their children safe

**3. Communication of Policy**

**3.1 Staff:**

All staff will be given the setting’s E-Safety Policy and its importance explained.

Staff should be aware that Internet traffic can be monitored and traced to the individual user and that discretion and professional conduct is essential.

**3.2 Parents:**

Parents’ attention will be drawn to the Setting’s E-Safety Policy in newsletters and on the Setting’s website. They will receive annual updates on E-Safety on our website

**4. Review**

This e-Safety Policy and its implementation shall be reviewed annually.

**5. The Internet**

The Internet is an essential element for education, business and social interaction. Internet use is a part of the curriculum and a necessary tool for staff and children and so the setting provides quality of Internet access as part of their learning experience. There are many risks, however, associated with abusive and dangerous web material that is easily accessible.

The Setting will ensure that:

* Internet access will be designed for child use including appropriate content filtering.
* The use of Internet derived materials by staff and pupils complies with copyright law.
* The setting meets the needs of all children and all teaching staff and our Inclusion. Leaders ensure all children have equal access to succeeding in this subject.
* All staff read and sign the ‘Acceptable ICT Use Agreement’ before using any setting ICT resource.
* Only authorised equipment, software and Internet access can be used within the Setting.
* If staff or children discover unsuitable sites, the URL (address), time and content shall be reported to the teacher/team leader who will then report to the Headteacher, by recording the incident in an E-Safety log, which will be stored in the Headteacher’s office with other safeguarding materials.
* The E-Safety Log will be reviewed termly by the E-Safety Leader.

**6. Social Networking and communication**

Social networking Internet sites (such as Instagram, Twitter, Facebook, Snapchat) provide facilities to chat and exchange information online, but the online world is very different from the real one with the temptation to say and do things beyond usual face to face contact.

The Setting will ensure that:

* All staff are aware that use of social networking sites and newsgroups in the setting is will be blocked/filtered and not used for personal use
* Parents, children and staff will be advised of the dangers of discussing children, staff or the setting on social networking sites.
* The Governors will consider taking legal action, where appropriate, to protect children and staff against cyber bullying and defamatory comments.
* Video conferencing will not be used without further consideration.
* Staff are not friends with parents on social networking sites

**7.** **Mobile Phones**

**a. NOT permitted**

* Staff will not have their private mobile phone on their person during work hours.
* Personal mobile phones and other photographic devices will be kept in a secure area away from where the children are accommodated.
* Staff may use their mobile phones during their designated breaks and in an area away from the children.
* The Setting’s contact number will be given as an emergency number in case practitioners need to be contacted.
* Reception staff need to ensure that visitor’s know they are not able to use their phones in the building or anywhere near children.
* Parents will be asked not to use phones while on the premises. If they need to use their mobile phone they will be asked to do so away from the children.

**b. Permitted use**

* In the setting, use of mobile phones will be for business and emergency purposes and practitioners are not to be distracted from the care of children.
* Staff must never exchange mobile phone numbers with parents in their setting (unless there is a specific purpose as stated below).
* Staff will be held responsible for the content and security of their own phones, e.g. access to web pages. If this is deemed to be a safeguarding issue this will be dealt with in line with the settings Safeguarding and management policies.
* Images taken of the setting or its children should be downloaded onto the Setting’s computer/laptop only. Images must not be downloaded onto any personal computer.
* Offsite on outings, mobile phones may be very useful. Where parent information is stored on a personal mobile for an outing this needs to be deleted after the outing is over. It is recommended for the senior member of staff to record this occurrence. Alternatively paper information may be taken on outings.
* All professionals should be reminded that that phone cameras, and photographs in general, can be used inappropriately, and the DSL or other staff will supervise and may veto, if necessary, the use of any mobile phone or camera within the vicinity of children on the Setting’s premises. All staff, regular volunteers and regular visitors using mobiles at the Setting will be asked to sign the ‘Acceptable Use ICT Agreement’. (Appendix 1)

**7.** **Digital/Video Cameras/Tablets**

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

The Setting will ensure that:

* Publishing of images, video and sound will follow the policy set out in this document under ‘Publishing Content’.
* Parents will not use digital cameras, mobile phones or video equipment at the setting unless specifically authorised by staff.
* The Headteacher or nominee will inform parents/carers and others present at events that photographs/videos may not be taken .

**8. Published Content and the School Website**

The Setting’s website is a valuable source of information for parents and potential parents but it must be managed to reduce any potential risks to families.

The Setting will ensure that:

* Contact details on the Website will be the setting’s address, e-mail and telephone number.
* Staff and children’s personal information will not be published particularly children’s names in association with photographs.
* The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
* Consent from parents will be obtained before photographs of children are published on the setting’s website

**9. Information System Security**

The Setting is committed to ensuring that all its ICTs are as secure as possible.

The Setting will ensure that:

* ICT systems capacity and security will be reviewed regularly
* Virus protection will be installed and updated regularly
* Security strategies will be discussed with Bristol City Council (BCC)
* E-Safety will be discussed with our ICT support and those arrangements incorporated in to our agreement with them.
* Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act.
* All reasonable precautions will be taken to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a Setting computer. The setting does not accept liability for the material accessed, or any consequences of Internet access. The setting will audit ICT use to establish if the E-Safety Policy is adequate and that the implementation of the E-Safety Policy is appropriate.

**13. E-Safety Complaints**

* Complaints of Internet misuse will be dealt with by a senior member of staff.
* Any complaint about staff misuse must be referred to the Headteacher.
* Complaints involving a safeguarding concern shall be dealt with in accordance with the Setting’s Safeguarding procedures.
* Parent/carers will be informed of the complaints procedure.
* Discussions will be held with the Community Police Officer to establish procedures for handling potentially illegal issues.

**14. Appendices**

Appendix 1 Acceptable Use of ICT Agreement

Appendix 2 Further Reading

 **Acceptable Use ICT Agreement**

ICT and the related technologies such as e-mail, the Internet, IPads and mobile phones are an expected part of our daily working life in the setting. This policy is designed to ensure that everyone is aware of their responsibilities when using any form of ICT. All users of IT within the Setting are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the setting’s E-Safety Co-ordinator, the setting’s E-Safety Leader is Morgan Hardy and the E-Safety Governor is \_\_\_\_\_\_\_\_\_\_\_\_\_

* I will only use the school’s e-mail/Internet/Intranet and any related technologies for professional purposes or for uses deemed ‘reasonable’ by the Headteacher or Governing Body.
* I will comply with the ICT system security and not disclose any passwords provided to me by the setting or other related authorities.
* I will ensure that all electronic communications with children and staff are compatible with my professional role.
* I will only use the approved, secure e-mail system(s) for any setting business.
* I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in the setting, taken off the setting’s premises or accessed remotely.
* I will not browse, download or upload material that could be considered offensive or illegal.
* I will not send to children or colleagues material that could be considered offensive or illegal.
* Images of children will only be taken and used for professional purposes and will not be distributed outside the setting’s network without consent of the parent.
* I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher.
* I will respect copyright and intellectual property rights.
* I will support and promote the setting’s e-Safety Policy and help children to be safe and responsible in their use of ICT and related technologies.

I agree to follow this code of conduct and to support the safe use of ICT throughout the setting.

Staff Signature…………………………………………….. Date………………………..

Print Name………………………………………………….

**Further Resources**

We have found these websites useful for E-Safety advice and information:

<http://www.ilminsterchildren.co.uk>

Our setting’s website for this and other policies and setting information

<http://www.bristol.gov.uk/page/children-and-young-people/bristol-safeguarding-children-board>

Bristol City Council’s Safeguarding Children’s Board site

<http://www.thinkuknow.co.uk/>

Set up by the Police with lots of information for parents and staff including a place to report abuse

<http://www.saferinternet.org.uk/>

The UK Safer Internet Centre, where professionals, parents and young people can find e-safety tips, advice and resources to help children and young people stay safe on the internet. The UK Safer Internet Centre is coordinated by a partnership of three leading organisations; Childnet International, the South West Grid for Learning and the Internet Watch Foundation. It is co-funded by the European Commission's Safer Internet Programme and is one of the 31 Safer Internet Centres of the Insafe network. The centre has three main functions: an Awareness Centre, a Helpline and a Hotline.

<http://www.childnet.com/>

Childnet is a UK-based charity set up to empower children, families and schools in the digital age. With the aim of making the internet a great and safe place for children, Childnet delivers internet safety workshops in schools across the UK to children aged 3-18, their parents, carers and teachers and also produces free educational resources for these audiences.

<https://www.getsafeonline.org/>

Get Safe Online is the UK’s premier source of information and advice for the public and small businesses on keeping safe and secure online. A joint initiative between the Government, National Crime Agency and other law enforcement agencies, and private sector organisations from the worlds of technology, communication, retail and finance, Get Safe Online offers free, impartial, easy-to-follow advice via its website, media and outreach activities and network of partners.