Brentry and Henbury
Children's Centres

E-SAFETY POLICY

At Brentry and Henbury Children's Centres e-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate professionals, parents/carers and children about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences and ensure their children are safe when using these technologies.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and service users; made explicit throughout policies.
- Sound implementation of e-Safety policy in both administration and curriculum, including secure network design and use.
- Safe and secure broadband, including the effective management of content filtering.

Internet Use
The purpose of Internet use in the Nursery and Centre is to raise educational standards, to promote achievement, to support the professional work of staff and to enhance management information and administration systems.

Internet use is a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for staff and parent/carers who show a responsible and mature approach to its use. Our Nursery and Centre has a duty to provide quality Internet access.

The benefits of using the Internet in education include:

- Access to learning wherever and whenever convenient
- Access to world-wide educational resources
- Educational and cultural exchanges world-wide
- Access to experts in many fields for parent/carers and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice
- Collaboration across support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates
- Collaboration of sharing child's learning and encouraging parent contribution
- Exchange of curriculum and administration data with the Local Authority and other bodies

It is acknowledged that, despite the benefits offered by the Internet, unlimited Internet use can have a detrimental effect the wellbeing of the Centre. Staff and parents/carers should therefore be taught what internet use is acceptable and what is not and given clear objectives for internet use. Internet access should be planned to enrich and extend learning activities for both parents and children.

All ICT resources at the centre have filtering systems which prevent access to unsuitable sites.

All staff must read and sign the confidentiality policy and key policies in induction process before using any ICT resource at the centre. All staff will be given the e-Safety policy and its importance explained during induction. Staff and parents/carers should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Any concerns that the internet is not being used appropriately will lead to the management team investigating and if necessary referring to the Trustees. If staff and parents/carers discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the management team.

The management team and Trustees will ensure that the use of internet derived materials by staff and parents/carers complies with copyright law. Staff and parents/carers should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy. The centre will work to ensure filtering systems are as effective as possible.

Email
Staff and parents/carers must immediately tell the management team or Trustees if they receive offensive e-mail. E-mail sent to external organisations should be written carefully and ensure that it encompasses accurate detail with name, title and organisation. Emails must abide to confidentiality policy and be written in a professional manner. The forwarding of chain letters is not permitted.

Mobile Phones
Ground rules are explored in groups regarding parent's use of mobile phones during groups. Guidelines of using mobile phones are placed in each community room. These rules are routinely explored with parents by staff. There is a strict no mobile phone policy in day-care rooms.

Social Networking
Brentry and Henbury Children's Centre should block/filter access to social networking sites and newsgroups unless a specific use is approved. Staff will be advised to read our social networking policy and to not 'friend' parents/carers or talk about the children centre unless promoting our social media page. Staff and parents/carers should be advised not to place centre photos on any social network space. Any photos displayed will be done through our business page where we will have obtained permissions to use photos.

Managing emerging technologies
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out by the management team before use is allowed.
Brentry and Henbury Children's Centre website
The contact details on the website will be the address, e-mail and telephone number. Personal information will not be published. The management team and the administrator will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing children's' images and work
Photographs that include children will be selected carefully and will be appropriate for the context. Parents/carers and children's full names will not be used anywhere on the Website, particularly in association with photographs. Written permission from parents/carers will be obtained before photographs of children are published on the Centre website. Work can only be published with the permission of parents/carers.

Tapestry
Parents/carers consent is given to upload photographs and information regarding their child to Tapestry (On line learning journal). We provide an email for them to set up a secure password to access their children's information. We ensure every parent signs to agree to treat photographs containing images of other children for their own personal use only, this means that the information cannot be shared with others or published in any way, without the explicit consent of the parents or carers of those children who may be included. For example any such photographs cannot be posted on social networking site or displayed in a public place.

Information system security
Centre ICT systems capacity and security will be reviewed regularly. Virus protection will be installed and updated regularly. Security strategies will be discussed with BCC and IT maintenance by the management team as necessary.

Protecting personal data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Assessing risks
The Centre will take all reasonable precautions 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 centre computer. We cannot accept liability for the material accessed, or any consequences of internet access. We will audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate.

Handling e-Safety Complaints
Complaints of Internet misuse will be dealt with by the management team. Complaints about abuse must be dealt with in accordance with Child Protection procedures. Parents/carers will be informed of the complaints procedure.

Parents/carers info
Parent/carers attention will be drawn to the e-Safety Policy in newsletters, the Parent Pack and on the website. As a centre we will aim to offer information sessions around e-safety to parents three times in an academic year.

Monitoring
The management team and trustees will monitor the use of computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of computer system may be taking place, or if the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.