Bristol Children's Playhouse
Growing Together

Online safety policy

Policy statement

Bristol Children's Playhouse accepts that in the 21st century the internet and social media are inherent to people's lives, important for sharing information as well as a learning tool. However, we are also aware that this global network comes with its own risks and dangers. We therefore set out the following guidelines to protect the children, staff and parents who use the setting.

Bristol Children's Playhouse has a commitment to keeping children safe and healthy and the Online safety policy operates under the umbrella of the Safeguarding Policy and is the implementation of the Safeguarding Policy in respect of electronic communications of all types.

Introduction

The Internet is now an essential resource to support teaching and learning, therefore it is important for children to learn to be safe online from an early age; our setting can play a vital part in starting this process. Digital skills are vital to accessing life-long learning and employment. Many children will use the internet outside of the setting and need to learn how to keep safe on the internet. Staff have a responsibility to help children stay safe online both in and outside of the setting.

- **How we use the Internet to enhance learning**
  Internet access is planned to enrich and extend children's learning activities. Staff will help guide the children with online activities to support the learning outcomes for their stage of development.
- **How children will be using the ICT equipment**
  It is unfortunate that children may be confronted with inappropriate materials, despite all attempts at filtering the internet. Staff will oversee children to ensure they can see any electronic device's screen so that they can intervene when necessary.
- **How staff will support children to understand the online risks they may face**
  Staff will work with children to develop an understanding of the online risks they may face, discuss and provide tools strategies and information to the children (or signpost them to where to get it) and also to their parents/ carers. The setting will develop/adopt key online safety messages to support this work.

1. Core Principles of Online Safety
The internet is as commonplace as the telephone or TV and its effective use is an essential life-skill. Unmediated internet access brings with it the possibility of placing children in embarrassing, inappropriate and even dangerous situations.

• Guided educational use - Significant educational benefits should result from internet use. This should be carefully planned and targeted within a regulated and managed environment.

• Risk assessment - We have a duty to ensure children in the setting are not exposed to inappropriate information or materials. We also need to ensure that children know how to ask for help if they come across material that makes them feel uncomfortable.

• Responsibility - Internet safety in the setting depends on staff, parents, carers and visitors taking responsibility for the use of internet and other communication technologies such as mobile phones. It is the setting's responsibility to use technical solutions to limit internet access and to monitor their effectiveness.

2. Why is it important for children to access the internet?
The internet is an essential element in 21st century life for education, business and social interaction. The setting has a duty to provide children with quality internet access as part of their learning experience and support them to learn appropriate internet use.

Our setting's internet access will be tailored expressly for educational use and will include appropriate filtering. Children will learn appropriate internet use. Staff will guide children with online activities that will support their learning and play journeys.

The internet is also used in the setting to support the professional work of staff, to allow effective planning and to enhance the setting's management information and business administration systems.

3. How will filtering be managed?

- The setting's staff/committee/management will ensure that the appropriate filters are applied to the electronic devices in the setting and to the electronic devices used by staff. They will also review/monitor the sites accessed on a regular basis.

- Children's electronic devices in the setting will have parental controls as well as internet security and virus protection. This will reduce children accessing sites of an unsuitable content when using the electronic device. Anything that appears unsuitable or offensive will be brought to the manager's/Online Safety Lead's attention which will then trigger appropriate action and be recorded as an incident. ***NOTE****: Many Internet Service Providers (ISP's)s offer a filtered service as well as putting filters and controls on the devices*

- Staff will monitor the websites being used by the children during sessions. If staff or children discover unsuitable sites have been accessed on the setting's electronic devices, they must be reported to the appropriate person immediately so that filters can be reviewed.

- There will be a named lead for reporting online incidents, overseeing internet use, training staff and developing online safety strategies for children and parents. This person will work closely with the Designated Safeguarding Lead.

- Our management will ensure there is sufficient funding and time made available for staff training to use systems.

- The setting will seek guidance from expert agencies to ensure safety arrangements are kept up to date:
  UK Safer Internet Centre;
  South West Grid for Learning – Early Years Toolkit.

4. How Internet access will be authorised

All sites that children have access to, will be used and viewed by the staff members before the children access them and they will be age appropriate and relevant to their learning.
Parents accessing their child's personal online learning journal accounts from home will use their personal emails and passwords that have been set up by the manager/setting.

5. Managing content and Information systems

It is important to review the security of the whole ICT system to keep everyone safe. All ICT equipment is checked at the beginning of each academic year and thereafter is checked regularly. The security of the setting's internet is protected by Web Root. All electronic devices have virus protection installed and are updated regularly.

Staff are responsible for ensuring that material accessed by children is appropriate and for ensuring that the use of any internet derived materials by staff or by children complies with copyright law.

The point of contact on the setting website should be the setting address, setting e-mail and telephone number. Staff or children's home information will not be published.

Website photographs that include children will be selected carefully and will not allow individual children to be clearly identified. Children's full names will not be used anywhere on the website, particularly in association with photographs. Written permission from parents or carers for featuring their child on the website is requested when each child starts at the setting and parents/carers wishes are followed. Parents may change this consent at any time by contacting the setting.

6. Communication

Managing email: Email is a useful way to communicate with parents about current activities and events in the setting.

- Email login details are known to the manager and deputy manager; they are not shared with other members of staff to ensure confidentiality.
- Staff using email will use a setting email address.
- All emails sent to parents are via the settings email address and never from a private/personal email address. When sending emails all email addresses are kept private. When sending out bulk emails to parents, the email addresses of other parents will never be displayed.
- The setting's email address must not be used for personal email.
- Children will not have access to email.

7. Helping children keep safe online

Staff have a responsibility to help children stay safe online both in and outside of the setting.

- By supporting children to develop their own understanding of the online risks they may face
- How to prevent or reduce risks
- How and where to get help and support.

The setting will develop an online safety strategy for children and their parents and carers.

8. Parents and online safety

Parent's attention will be drawn to the settings online safety policy. We will do this by using our Parentmail system.

- While on the premises parents/carers will be asked to comply with the settings mobile phones and online safety rules.

9. Staff use of the setting's electronic devices

- Staff will not use the setting's electronic devices for personal use.
- The setting will ensure that all programs used and websites accessed are appropriate and that children are not able to access or download material which is unsuitable.
- All setting files that contain personal data will be stored appropriately and securely, e.g.: password protected or locked away.
- Staff will not forward any of the setting's work, files, information etc stored on the setting's electronic devices to their personal electronic devices, unless this has been agreed and recorded by management as necessary. Any work taken home will be protected as if it were in the setting and open to scrutiny by management.
- Staff will not use any personal memory devices in the setting's electronic devices. Memory sticks provided by the setting will be used for work purposes only and will be kept securely.
- Generally, all ICT equipment should remain in the setting. This is to minimise the risk of computer viruses and for data protection purposes.

- Staff will not access, copy, remove or otherwise alter any other user's files, without their expressed permission.
- All email communication will be appropriate and written in a professional manner.
- Illegal or inappropriate materials MUST NOT be uploaded, downloaded or accessed.
- Staff will ensure that setting's electronic devices are used appropriately to avoid disabling or damaging equipment.

10. Social Networking/Media Sites

Social networking sites (e.g. Facebook, Twitter and Instagram) can be a useful. Advertising tool for settings and can often be an effective way of engaging with young or hard to reach parents. Due to the public nature of social networking and the inability to keep content truly private, great care must be taken in the management and use of such sites

- Staff, volunteers, students, registered bodies etc will/should not put details of their work on any form of social networking site.
- To maintain professional distance and to avoid unwanted contact, staff should not link their personal social networking accounts to the setting's page.
- No staff are permitted to 'friend' parents/carers currently accessing the setting. New staff starting with the setting will be asked to defriend these people. A safeguarding message is available on request explaining the reason for defriending if required. Or staff will declare any pre-existing friendships with parents/carers to the manager and commit to keeping strict work /life boundaries.
- Staff, volunteers, student, registered bodies etc should not engage in any on-line activity that may compromise their professional responsibilities.
- Staff, volunteers, student, registered bodies etc must be very cautious about the content they post online. Everyone in the setting must be mindful that once content is placed online, even if swiftly removed, can remain out in the ether accessible to all.
- All staff, volunteers, students etc are to adapt their privacy settings to ensure that only friends can see their personal social networking profiles. In the case of social media sites where you cannot control who sees the content please see point above.
- Photographs, names of, or comments about children within the setting must never be placed on any social networking site.
- Adults working with children/young people should not correspond with setting's children/families through social networking sites.
- Staff will not discuss individual children or their setting on any social networking site.
- Staff should be aware of possible professional implications/risks when entering any personal details on any gaming or social networking sites (e.g. YouTube, Facebook, twitter etc).
- Staff will not be permitted to use the setting's electronic devices to access social networking sites at any time, including designated breaks.
- All communications in the setting will be transparent and open to scrutiny.
- If staff or children discover unsuitable sites, the URL (address) and content must be reported to the Manager or named Online Safety Lead. This will be recorded.

- All staff must be made aware that failure to comply with policies and procedures may result in disciplinary action being taken.

11. Children's use mobile phones/devices

Whilst we are limited in our use of devices at the setting, it is important to recognise that children may have access to phones or tablets at home.

- Staff will signpost parents to information on how to set up, filter and control their child's device to reduce the risk of them accessing harmful online material.

12. GDPR

Bristol Children's Playhouse understands that we have a duty to comply with the General Data Protection Regulations (GDPR). To do this we will research our responsibilities (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/) and fulfill them according to the type and size of our organisation.

The Information Commissioner's Office has condensed the Data Protection Principles into six definitions, which are referred to as the Privacy Principles. They are:

1. You must have a lawful reason for collecting and processing personal data and must do it in a fair and transparent way. There are six lawful reasons for doing this – see www.ico.org.uk
2. You must only use the data for the reason it is initially obtained.
3. You must not collect any more data than is necessary.
4. It has to be accurate and there must be mechanisms in place to keep it up to date.
5. You cannot keep it any longer than needed.
6. You must protect the personal data.

These privacy principles are supported by a further principle – accountability.
BCPH pays an annual subscription to be a member of the ICO and commits to adhering to the principles outlined above.

We will endeavour to train all staff on data protection where appropriate and possible.

13. Handling Complaints

Any complaints about the appropriate use of the internet or other technologies will be handled through the setting's complaints procedure.

14. Named lead for Online Safety is Kirsty Clark

Further Information

South West Child Protection Procedures – provide detailed online information on all aspects of child protection : https://www.proceduresonline.com/swcpp/

Data Protection – Information Commissioners Office, detailed information on all aspects of data protection: https://ico.org.uk/

Internet Matters – Helping parents keep their children safe online: www.internetmatters.org

Common Sense Media - reviews information and age ratings on all sorts of media: https://www.commonsensemedia.org/

South West Grid for Learning
https://swgfl.org.uk/online-safety/
https://swgfl.org.uk/resources/early-years-toolkit/

UK Safer Internet Centre
https://www.saferinternet.org.uk/

POSH (Professionals Online Safety Hotline) https://www.saferinternet.org.uk/our-helplines
Monday to Friday 10:00am – 4:00pm
For help and support, please email helpline@saferinternet.org.uk