

**E-Safety policy**

**Statement of Intent**

Brislington Village Pre-School 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. This policy operates at all times under the umbrella of our Safeguarding policy.

**Aims**

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. Our aim is to begin the learning process for our children on how to be e-safe, to recognise when information or material is inappropriate or makes them feel uncomfortable and how to ask for help.

Our aim for our staff is for them to be protected when using any form of ICT including the internet.

**Methods**

Our named E-safety officer is April Blackmore.

* **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.

**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.

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.

The setting’s management and E-safety officer 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.

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.

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 admin/manager/setting.

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.

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.

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.

Parent’s attention will be drawn to the settings online safety policy. We will do this when a child begins by drawing attention to the parent/carer of our policies which are available on our website. A printed copy is available anytime on request. While on the premises parents/carers will be asked to comply with the settings mobile phones and online safety rules.

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.

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, 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

Staff, volunteers, student, etc should not engage in any on-line activity that may compromise their professional responsibilities.

Staff, volunteers, student, 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 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.

This policy was adopted at a meeting on 23 May 2016

Reviewed September 2021

This policy should be read in conjunction with our:-

Photography, video, mobile phone and social networking policy

Safeguarding children policy

Staff Behaviour policy

Although under constant review, an overall review date has been set for **September 2022**

**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](http://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](mailto:helpline@saferinternet.org.uk)