Policy and Procedures

Acceptable use & digital safety policy

We recognise the exciting opportunities technology offers to staff and children in our school and have invested in age-appropriate resources to support this belief. While recognising the benefits we are also mindful that practitioners have a duty of care to ensure that children are protected from potential harm both within and beyond the physical and virtual boundaries of our school.

To reflect our belief that when used appropriately and safely, technology can support learning, we encourage adults and children to use a range of technological resources for a wide range of purposes. At the same time, we do all we can to ensure that technology is used appropriately and that children are safeguarded against all risks. While it is not possible to eliminate risk, any e-safety concerns that do arise will be dealt with quickly to ensure that children and staff adhere to safe practices and continue to be protected. We will communicate our safe practice in the use of technologies with families and manage any concerns.

Scope of the policy

This policy applies to everyone- staff, children, parents/carers, visitors and contractors accessing the internet or using technological devices on the premises. The policy is also applicable where staff or individuals have been provided with school issued devices for use off-site.

We aim to:

- Raise awareness amongst staff and parents/carers of the potential risks associated with online technologies, whilst also highlighting the many learning and social benefits
- Maintain a safe and secure online environment for all children in our care.
- Provide safeguarding protocols and rules for acceptable use to guide all users in their use of technology and online experiences
- Ensure all adults are clear about sanctions for misuse of any technologies both within and beyond the early years school.

Hardware and provision use

Where staff have been issued with a device (e.g. school laptop or iPad) for work purposes, personal use whilst off site is not permitted unless authorised by the provider/Headteacher. The schools' laptop/devices should be used by the authorised person only. Only technology owned by the school will be used on the premises and on school visit or outings. This includes mobile devices for everyday use, and, in case of emergency, a mobile phone is provided. Staff taking photographs or recording with technology not owned by our school is specifically not allowed.

All staff have a shared responsibility to ensure that children are supervised when using the internet and related technologies to ensure appropriate and safe use as part of the wider duty of care and responding or reporting promptly to issues of concern.

School issued devices only should be used for work purposes and, if containing sensitive information o, should not leave the premises unless encrypted

Online searching and installing/downloading of new programs and applications is restricted to authorised staff members only. Children should not be able to s install anything on a school device.

Next review: Michaelmas 2025
Reviewed: EW/RC

Data storage and management

All data relating to children or staff is stored securely on ISAMS No electronic documents that include children's names or digital images will be transported out of the school e.g. on Fobs, memory sticks.

Email

School staff have access to a professional email account to use for all work related activities, including communication with parents/carers. This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.

Staff should not participate in any material that is illegal, obscene and defamatory or that is intended to annoy or intimidate another person or persons.

All emails should stay professional in tone and checked carefully before sending, just as an official letter would be. Care should be taken when forwarding emails from others.

Social Networking

Employees must not access personal blogs/social networking sites on work devices without prior agreement or in accordance with the school's policy.

The school does not condone employees writing about their work on social networking sites or web pages. If employees choose to do so, they are expected to follow the rules below.

Staff use of social media:
We require our staff to be responsible and professional in their use of social networking sites in relation to any connection to the school, school staff, parents or children.

- If a parent ask questions relating to work via social networking sites, then staff should reply asking them to come into the school or contact the Headteacher.
- Ensure any posts reflect their professional role in the community (e.g. no inappropriate social event photos or inappropriate comments i.e. foul language)
- Report any concerning comments or questions from parents to the Headteacher/safeguarding lead.

Remember that anything posted online could end up in the public domain to be read by children, parents or even future employers – so staff should be mindful of this when posting comments or photos. For example, posting explicit pictures of yourself could damage your reputation and that of your profession and organisation. Parents and employers may also question your suitability to care for children.

Staff must not:

Next review: Michaelmas 2025
Reviewed: EW/RC

- disclose any information that is confidential to the school or any third party or disclose personal data or information about any individual child, colleague or service user, which could be in breach of the Data Protection Act.

- link their own blogs/personal web pages to the school's website.

- make defamatory remarks about the school, colleagues or service users.

- misrepresent the school by posting false or inaccurate statements.

- not post anything that could be construed to have any impact on the school's reputation or relate to the school or any children attending the school in any way.

If any of the above points are not followed then the member of staff involved will face disciplinary action, which could result in dismissal.

Communication with children and young people, by whatever method, should always take place within clear and explicit professional boundaries. Staff should avoid any misinterpretation of their motives or any behavior that could be construed as grooming.

Social Media:

We use social media to share pictures of the children within school. In order to safeguard children, we will:

- Ensure all children in the photographs or posts have the correct permissions in place from their parent.
- Monitor comments on all posts and address any concerns immediately.

Sanctions

Misuse of technology or the internet may result in:

- the logging of an incident
- disciplinary action
- reporting of any illegal or incongruous activities to the appropriate authorities
- allegations process being followed

Next review: Michaelmas 2025
Reviewed: EW/RC