E-Safety Policy

At Edinburgh Montessori Arts School we provide a diverse, balanced and relevant approach to the use of technology. Children are encouraged to maximise the benefits and opportunities that technology has to offer. Children learn in an environment where security measures are balanced appropriately with the need to learn effectively.
This policy sets out our commitment to safeguarding children, staff and families in their use of online technologies. It addresses the responsibilities of all staff, volunteers, visitors and parents in using online technologies safely and outlines the reporting procedures should an incident occur.

Roles and responsibilities
E-safety is everyone's responsibility. We have a designated lead person for e-safety who oversees the management of online safety of all users and ensures that it is agreed and respected by all. The role of the designated e-safety lead includes:

- ensuring that the e-safety policy and associated documents are up to date and reviewed regularly
- ensuring that the policy is implemented and that compliance is actively monitored
- ensuring that all staff are aware of reporting procedures and requirements should an e-safety incident occur
- ensuring that the e-safety incident log is appropriately maintained and reviewed regularly
- ensuring that children are supported to learn about online safety in a way that is appropriate for their age and development
- keeping up to date with e-safety issues and guidance
- ensuring e-safety updates, training and advice is available for staff, parents/carers
- liaison with the designated safeguarding lead to ensure a co-ordinated approach across relevant safeguarding issues.

All staff have a shared responsibility to ensure that children are able to use the internet and related technologies appropriately and safely as part of the wider duty of care to which all adults working with children are bound.

Training

Staff are trained to follow best practice when using online technologies, and the training needs of staff are identified. There is a planned programme of online safety training for all staff with induction and regular updates that support safeguarding practice. The availability of internal and external training is advertised to staff.

Reporting

The culture of the organisation encourages all staff and users and its wider community to be vigilant in reporting issues. There are clear and understood systems for reporting e-safety incidents and concerns to management, and there are clear escalation processes for the handling of incidents. Issues raised will be dealt with quickly and sensitively. Reports of incidents are logged and regularly audited and monitored. There are good links with outside agencies.

Sanctions

The organisation is strict in monitoring and applying the e-safety policy. Staff and users are made aware of the consequences of their actions should they misuse online technologies. Incidents of misuse will be dealt with through accepted disciplinary procedures, which may include verbal or written warning, suspension, referral to local authority, and/or referral to police. Users are informed that sanctions can be applied to e-safety incidents that take place outside of the organisation if they are related to the organisation.

Filtering and Supervising

The provision ensures that there is safe access to the internet. An accredited or approved Internet Service Provider, (ISP), is used to provide internet access and there is an effective age-appropriate filtering system combined with user discussion and consistent supervision. Reporting of inappropriate sites is to the e-safety lead who logs them.

Email Use

The provision provides all staff with access to a professional email account to use for all work-related business, including communication with parents and 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. All emails should be professional in tone and checked carefully before sending, just as an official letter would be. Email is covered by the Data Protection Act (2018), the Freedom of information Act (2000) and the General Data Protection Regulation so safe practice should be followed in respect of record keeping and security.

Use of Social Networking Sites

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. Identifiable images of children are not be used on social networking sites. To maintain professional distance and to avoid unwanted contact, staff should ensure that their own social networking accounts are set to private. Privacy settings are set to maximum and checked regularly.

Mobile phones

The provision allows staff to bring in personal mobile phones and devices for their own use but under no circumstances can a member of staff use a device while working. Users bringing personal devices into the provision must ensure that there is no inappropriate or illegal content on the device. The provision is not responsible for the loss, damage or theft of any personal mobile device.

Photographs and digital images

There are strict policies and procedures about the use of digital imagery and videos, which are covered in our Digital Images policy. The provision seeks to minimise risks involved in the taking, storing, using, sharing, publishing and distribution of digital images and video. There are well-established procedures for gaining parental permission and consent is sought every 12 months. Standards are rigorously applied by all users and reviewed in the light of changing technologies.

Laptops, computers and tablets

Where staff have been issued with a device for work purposes, personal use while offsite is not permitted unless authorised by the Principal. The provision's laptop/devices should be used by the authorised person only. Staff are aware that all activities carried out on the provision's devices and systems, both within and outside of the work environment, will be monitored in accordance with this policy. Devices used by staff and users are protected from viruses, hacking, etc and are regularly updated and password protected. All staff and users have individual passwords that are strong and regularly updated. Staff will ensure that provision laptops and devices are made available as necessary for anti-virus updates, software installations, patches, upgrades or routine monitoring/servicing.

Children's use of computers and tablets must be supervised by an adult at all times, and any games or apps used must be from a pre-approved selection. Online searching and installing/downloading of new programmes and applications is restricted to authorised staff members only.

Personal staff tablets or laptops should not be used for any apps that record and store children’s personal details, attainment or photographs. Only devices belonging to the provision may be used for such activities, ensuring that any devices used are appropriately encrypted if taken off site.

Data storage and security

Personal data is safe and secure. It is understood by all staff and users and this ensures the safekeeping of personal data, minimising the risk of loss or misuse. The organisation has a Personal Data policy and staff understand the need to ensure the safekeeping of personal data.

Reviewing practice

The organisation regularly reviews its practice in the light of emerging new technologies to ensure all users are safeguarded online. A record of the review is kept by the e-safety lead. Incident logs and monitoring reports are recorded.