



Policy reviewed on 20.09.2017

Online Safety Policy

Aim: To enable adults and children to communicate and learn to use ICT safely.

The Exwick Ark recognises the immense value of ICT to adults and children's learning and communication but also that there are risks involved. This policy seeks to minimise these risks whilst maximising the benefits. Paula Stone and Harriet Sharp (designated safeguarding officers) are responsible for ensuring that this policy is put into practice.

Acceptable use of internet.

Internet access by staff at work is restricted to those sites which are necessary for their professional duties. Website history on the work laptop is checked by our safeguarding officers. Websites selected to use with children are always appropriate for their age and stage of development and children's online use is continually supervised by staff. Secure passwords are used at all times to access the laptop. Up to date virus checkers and security are built into any form of technology used to access the internet (computers, phones and games consoles.) If any potentially unsafe or inappropriate incident should take place it should be reported immediately to our designated safeguarding officers who will take any necessary action. Photographs are stored on our Onedrive system, Elitepathway and displayed on our Facebook pages, with permission of parents, and this is registered with data protection.

Social networks.

The use of social networking sites by staff is not permitted during work hours. Staff must never discuss children, staff or parents when using public areas of social networking sites. Full names of children or parents should never be used even on private chat. If using the private chat function to discuss a work issue the dialogue box should always be cleared before closing down. Staff are strongly advised not to become online friends with parents on social networking sites. This practice is regarded as highly unprofessional and a risk to staff member's own privacy. Any breach of confidentiality, or abuse of staff, parent or child on a social network site will be regarded as gross misconduct and may result in instant dismissal. Any abuse of these sites reported must be recorded and dealt with immediately by our safeguarding officers. Use of Exwick Ark's Facebook page is used to advertise and communicate with parents. Posts on this page are regularly monitored by our safeguarding officers and any breaches of confidentiality or abuse should be reported immediately.

Use of cameras

Personal cameras must not be used within the setting. Only an authorized setting camera should be used to take images.



Parental permission is sought to take still and moving images of children during the initial registration and termly updates.

Each family worker group has access to a digital camera or a tablet. This camera should be easily accessible to capture spontaneous moments to support the observation requirements of the EYFS and to share with parents.

The play leader at the end of the day is responsible for checking all cameras are present as part of the closing checks. Any missing cameras should be reported to the designated safeguarding officer.

Memory cards are removed from the cameras and stored separately.

When taking a memory card or storage device off site it should be logged in and out in the communication book by the designated safeguarding officer and monitored carefully to ensure it is returned within the expected timescale.

Students wishing to take photographs as part of a project should use work cameras and print the photographs off at the setting whenever possible. If they use their own camera they should only take photographs of the building without children being included.

Mobile phones

Personal mobile phones are not permitted in areas occupied by children and should be left in the staff room or locked in the filing cabinet if preferred.

Use of personal mobile phones are restricted to lunch or tea breaks unless in unusual circumstances it had been agreed by the designated safeguarding officer. Any unauthorised use of mobile phones whilst children are present must be reported, monitored and recorded. The recording or sharing of images, video clips or audio material on any mobile phone is prohibited except where it is explicitly authorized by the designated officer for safeguarding. All mobile phones must be open to scrutiny and the designated officer for safeguarding has the right to withdraw or restrict their use further if at any time it is deemed necessary.

The use of a work mobile is considered to be an effective communication tool. It will enable work related text, e-mail messages and calls to be made and received. It is an essential part of the emergency kit when going out on outings. It can also provide essential back up if landline services are unavailable or when contact needs to be made out of hours. The work mobile should only be used for authorised work purposes and is not for personal use unless agreed by the designated safeguarding officers.

ICT Misuse.

All incidents of suspected misuse of ICT should be reported to the designated safeguarding officer immediately. These incidents will be recorded and investigated and dealt with according to the procedures outlined in our safeguarding and disciplinary policies.

20th September 2017

Signed: