



## **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.

### **Legislation and non statutory Guidance**

Early Years Foundation Stage.

Statutory guidance "Working Together to Safeguard Children" 2018

Non statutory Guidance "Keeping Children Safe in Education. 2018

Non Statutory Guidance Safeguarding Children and Protecting Professionals in Early Years Settings Feb 2019

Online Safety Guidance for Practitioners.

### **Roles and Responsibilities.**

#### **Designated Safeguarding Officers**

Our designated safeguarding officers at each setting are trained in Online Safety issues and aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate online contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

Our managing directors are responsible for ensuring this policy is implemented and monitored and that staff are given appropriate training.

#### **Staff**

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the Exwick Ark Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the *Designated Safeguarding Officer* for investigation.
- They model good online safety for children, for example, asking for permission to take their photo even if they have parental consent.



### **Parents / Carers**

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The *Exwick Ark* will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature*. Parents and carers will be encouraged to support us in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at our events
- access to parents' sections of on-line pupil records

### **Training**

Our Designated Safeguarding Officers access training and information to ensure they understand the unique risks associated with online safety for early years children and have the up to date capability required to keep children safe online.

Managers ensure that staff are provided with quality and up to date online safety training on a regular basis (at least annually) and at induction.

Parents are given opportunities to develop their knowledge of online safety issues for early years children and are offered support to help them talk to their children in an age appropriate way. We sign post parents to appropriate sources of support regarding online safety at home.

### **Technical Systems**

- Exwick Ark technical systems will be managed in ways that ensure that we meet recommended technical requirements.
- There will be regular reviews and audits of the safety and security of Exwick Ark technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to Exwick Ark technical systems and devices.
- All staff will be provided with a username and secure password by Harriet Sharp *who will keep an up to date record of users and their usernames*. Users are responsible for the security of their username and password *. It must be checked as being a secure password*. The “master / administrator” passwords for Exwick Ark ICT systems, used by the Network Manager are also available to the *Harriet* and kept in a secure place.
- Harriet is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users.



- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.

### **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 laptops, ipads and desk top computers is checked by our safeguarding officers.

Websites selected to use with children are always appropriate for their age and stage of development. When activities are pre planned staff check apps, websites and tools prior to using them with children, this includes checking the results of searches. Appropriate filters and monitoring systems are in place to protect learners from potentially harmful online material. Children's online use is continually supervised by staff. Children are reminded to tell an adult about anything that makes them feel worried when using technology. Staff model safe practice when using technology with children.

We make use of home visits to inform our understanding of a child's context with regard to technology within the home e.g. how much and in what ways technology is used within the child's family life.

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. Civil, legal or disciplinary action can be taken against staff if they have brought the setting into disrepute. Under no circumstances should a member of staff, either at work or in any other place, make, deliberately download, possess, or distribute material they know to be illegal.

Photographs are stored on our Onedrive system, Elitepathway and displayed on our Facebook pages, with permission of parents, and this is registered with the Information Commissioner's Office.

### **IPAD's**

In our settings all staff have access to an Ipad connected to the wifi when working in the room with the children. Staff are regularly reminded about only using this to access sites appropriate to their work with children. Search history is regularly checked by our safeguarding officers. Staff use these Ipads to take observation photos and upload them to our secure online record keeping system. They use them to access our Office 365 and Childsplay software and to research information on websites with children. Staff may not remove these devices from the setting and they are stored in a locked cupboard over night. They are protected with a secure password and screen lock. Appropriate filtering systems are in place. Playleaders are responsible for collecting Ipads at the end of the day and safe guarding officers should be noted if any are missing.

### **Personal data online.**



Personal data online is managed securely in accordance with the statutory requirements of the General Data Protection Requirements and Data Protection legislation. Further details of this can be found in our GDPR file.

### **Use of digital and video images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and carers need to be aware of the risks associated with publishing digital images on the internet. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. Exwick Ark will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- Written permission from parents or carers will be obtained before photographs of pupils are published on our website / social media / local press.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at Exwick Ark events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *children* in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow our policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Exwick Ark equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the nursery into disrepute.
- Children must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.
- Children's full names will not be used anywhere on a website or blog, particularly in association with photographs.



### **Data Protection**

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The Exwick Ark:

- Has a Data Protection Policy.
- Is registered with the Information Commissioner's Office (ICO).
- Has named Harriet Sharp as the Data Protection Officer (DPO).
- Will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Ensures data held is accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Has procedures in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- Has data retention policies and routines for the deletion and disposal of data.
- Has a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data. A secure password has at least 8 figures and consists of a combination of numbers, symbols and upper and lower case letters.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:



- The data must be encrypted and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device once it has been transferred or its use is complete.

### **Communication Technology**

- The official Exwick Ark email service may be regarded as safe and secure and is monitored.
- Users must immediately report, to the nominated person the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school / systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Personal information should not be posted on the Exwick Ark website and only official email addresses should be used to identify members of staff.

### **Online Learning Journeys**

Children's records are held securely online using the Elite Pathway website. Data on here is password protected, accessed only by staff and the child's parent and held securely according to the GDPR legislation.

### **Social networks.**

Staff are regularly reminded that they need to manage their digital reputation, including the appropriateness of information and content that they post online, both professionally and personally. No matter what privacy settings are used, anything posted online can become public and permanent and could be misinterpreted and /or used without their consent or knowledge. Staff should discuss online expectations and behaviour with their friends and colleagues – for example, the type of photos that can and cannot be posted of them on social media.

#### **Personal Use:**

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used in connection with The Exwick Ark or impacts on the Exwick Ark, it must be made clear that the member of staff is not communicating on behalf of the Exwick Ark with an appropriate disclaimer.



- Staff may not access personal social media sites in work hours where this is suspected, disciplinary action may be taken. Staff may access it at break times.
- **Staff must never discuss children, staff or parents when using social networking sites.**
- Staff are strongly advised not to accept friend requests or communications from pupils or their families (past or present) on social networking sites. This practice is regarded as highly unprofessional and a risk to staff member's own privacy. Pre-existing relationships should be discussed with the DSL who will need to consider how this is managed, provide staff with clear guidance and record actions taken.
- 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.

#### **Official Exwick Ark Social media sites:**

*Only senior leaders are able to publish to our social media sites and each page has at least 2 administrators. Paula Stone monitors these accounts.*

#### **Monitoring of Public Social Media**

- As part of active social media engagement we pro-actively monitor the Internet for public postings about The Exwick Ark

#### **Use of cameras**

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

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 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.

If work e-mail is accessed on a personal mobile phone the phone must be securely password protected or use a thumb print to unlock.

Use of personal mobile phones are restricted to lunch or tea breaks in the staff room 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.

#### Children's phones

Children will not need to use their phone whilst in the setting, therefore they should be given to a member of staff who will put them in the locked admin cupboard until they go home. At no point during the child's time with us will they be permitted to use it for taking photos, recording images or for accessing the internet, playing games or using social media.

### **Intelligent Speakers**

Intelligent speakers (Amazon Alexa's) are used in some rooms. These are linked to the Exwick Ark Amazon account. Settings are set to turn off skills unsuitable for children for example voice purchases. The history is regularly checked by our safeguarding officers to see the commands given. Microphones can be disabled when not in use. Children are always supervised when using the Alexa's. Alexas are positioned away from windows where they could be accessed by the public.

### **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.

It is hoped that all members of the Exwick Ark community will be responsible users of digital technologies, who understand and follow our policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.





**In the event of suspicion, all steps in this procedure should be followed:**

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority Designated Officer
  - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - promotion of terrorism or extremism
  - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

**It is important that all of the above steps are taken as they will provide an evidence trail and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.**

**Contacts.**



If we need to report an illegal image (child sexual abuse material) we can contact the Internet Watch Foundation. <https://iwf.org.uk/>

If we are worried about online abuse or the way someone has been communicating online we can contact the Child Exploitation and Online Protection Centre (CEOP) <https://www.ceop.police.uk/ceop-reporting/>

The UK Safer Internet Centre has a helpline for professionals <https://www.saferinternet.org.uk/professionals-online-safety-helpline>

The UKCIS framework(Education for a connected World) provides information about the skills and competences that children and young people need to have with regards to online safety from the age of 4 up.

This policy is updated annually and in response to local and national changes.

19.11.2019

Signed:



## **Staff (and Volunteer) Acceptable Use Policy Agreement**

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

*This Acceptable Use Policy is intended to ensure:*

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that Exwick Ark systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk. that staff are protected from potential risk in their use of technology in their everyday work.

The Exwick Ark will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for children and will, in return, expect staff and volunteers to agree to be responsible users.

### *Acceptable Use Policy Agreement*

I understand that I must use Exwick Ark systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that children receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

*For my professional and personal safety:*

- I understand that the Exwick Ark will monitor my use of the company digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, etc.) out of the setting, and to the transfer of personal data (digital or paper based) out of the setting.
- I understand that the Exwick Ark digital technology systems are primarily intended for educational use and that I will only use the systems for personal use within the policies and rules set down by The Exwick Ark.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.



*I will be professional in my communications and actions when using Exwick Ark ICT systems:*

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with The Exwick Ark policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on The Exwick Ark Facebook/Instagram page) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in the setting in accordance with The Exwick Ark policies.
- I will only communicate with parents and carers using Exwick Ark systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities.

*The Exwick Ark have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the business:*

- I will not use my personal mobile devices (laptops / tablets / mobile phones / USB devices etc) in the setting when children are present.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings without permission from my manager.
- Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or child data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.



*I understand that I am responsible for my actions in and out of The Exwick Ark*

- I understand that this Acceptable Use Policy applies not only to my work and use of digital technology equipment in the setting, but also applies to my use of Exwick Ark systems and equipment off the premises.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the Exwick Ark digital technology systems within these guidelines.

Staff / Volunteer Name:

Signed:

Date: