IT, Internet and Social Networking Policy

Windmill Under 5s, Lacey Green and Loosely Row Sports Club, Main Road,
Lacey Green, Princes Risborough HP27 0PL
Registered charity no: 1026976

Reviews and Approvals

Policy adopted :	17 January 2014 by Windmill Under 5s Management Committee	
Date of last review:	23 November 2020	
Date of next review:	Autumn Term (November) 2021	
Signed & dated:		Natasha Kann – Chairperson on behalf of the Management Committee

Information and Records: Providers must ensure that all staff understand the need to protect privacy of the children in their care as well the legal requirements that exist to ensure that information relating to the child is handled in a way that ensures confidentiality.

Child Protection

8. IT, Internet and Social Networking Policy

Policy statement

Windmill Under 5s takes steps to ensure there are effective procedures in place to protect children, young people and vulnerable adults as well as staff, committee members and parents from the unacceptable use of ICT (Information Communication Technology) equipment, or social networking or social media use.

Procedures

ICT Equipment

- Only ICT equipment belonging to Windmills is used by staff and children in the setting.
- The Preschool Manager and Business Manager are responsible for ensuring all equipment is safe and fit for purpose.
- The preschool laptop has virus protection installed.
- The preschool laptop, staff tablets and 'play' tablets used by the children, are located in an area visible to staff.
- All devices are password protected to prevent unauthorised access.
- Children are not permitted to bring in personal ICT equipment, including mobile phones. If a child is found with any devices, these will be removed and stored in the changing room until the parent/carer collects the child at the end of session.
- Equipment belonging to Windmills must not be used to access any websites containing adult content, neither should personal equipment containing this content, or links to them, be brought into Windmills.

Internet Access

- Whilst there is internet access within the preschool children are unable to access the internet via the devices that they have unsupervised access to. Children have access to 'play' tablets but the Wi-Fi function is disabled.
- Windmills' laptop computer used on the premises by staff, is only accessed by children when they are doing a specific activity with a member of staff. Therefore, children do not have unsupervised access to the internet.

- Staff members, as well as Management Committee members, will be using a range of technology resources to manage their roles as professionals at home. To do this they will most likely be using the internet to research and communicate professionally. They may use Tapestry to track and record progress of children and to communicate with parents/carers. They may also participate in professional forums, or manage administrative tasks. In all these areas, it needs to be remembered that the same professional standards are expected as those expected in the work place. As do the same confidentiality rules and standard of professionalism and working practice. Similarly, that any devices used to access preschool content have strong password protection and all attempts are made to prevent unauthorised access.
- All Management Committee members sign a Code of Conduct each year at the AGM to ensure they are aware of their responsibilities in this regard.
- All staff members sign a Code of Conduct at the time of the AGM to ensure they are aware of their responsibilities in this regard.

E-mail

- Children do not have access to e-mail.
- Staff do not access personal email whilst supervising children on the Windmills laptop or on the staff tablets.
- Any personal information relating to children or their families, which is forwarded to outside agencies by email is sent by encrypted or password protected email. Any information shared via USB is password protected.
- Staff are not to use personal email addresses to contact families or service users. Any communication via email with families or service users should be done via the Business Manager using the admin@windmillunder5s.co.uk address, the Preschool Manager using the manager@windmillunder5s.co.uk, SENDCo using senco@windmillunder5s.co.uk or Chairperson using the windmillschair@gmail.com address.

Using Personal Devices for Work

- This section applies to employees, volunteers and trustees, who use their own mobile telephones, tablets, personal laptops and/or PCs to access Windmills data; particularly confidential, sensitive or personal information in relation to employees, volunteers, children, families and other stakeholders.
- Allowing individuals to make use of their own device(s) for business purposes may result in the need for such devices to be subject to additional controls over and above those typically in place for a consumer device. Common issues and security challenges, as outlined below, must be considered when assessing the suitability of any given device to hold specific data belonging to the setting.

- Permission will only be provided for individuals to use their personal phones, tablets, laptops and PCs for work-related purposes, where there is a good business case and strict adherence to this policy. Approval must be sought from the Committee Chairperson.
- Employees may view sensitive personal data (defined under the General Data Protection Regulation (GDPR) as data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation) on a personal device only if the device has a sufficiently high level of encryption. However, sensitive personal data must not be stored on personal devices in any other way.
- Before using his/her own device for work-related purposes, an employee, volunteer, trustee must ensure that he/she uses a strong password to lock his/her device. The device must be capable of locking automatically and deleting data automatically. In addition, individuals must:
    - use encryption software on their devices to store personal data securely; ensure that they assess the security of any open network or Wi-Fi connection and ensure unsecured Wi-Fi networks are not used
    - have an up-to-date anti-virus program installed which runs regular scans of the system for unwanted and malicious services or programmes; where possible this should also provide internet filtering to prevent harmful sites from being accessed
    - not download unverified or untrusted apps that may pose a threat to the security of the information held on the device
    - not, under any circumstances, use Windmills personal information for any purpose other than for their work and as directed or instructed by the setting
    - ensure that they have a system of software in place for quickly and effectively revoking access that a user might gain to a device in the event of loss or theft; if possible this software should also allow remote wiping of data from the device
    - make sure that any software they use is genuinely installed under an appropriate license agreement with suitable support from the relevant manufacturer to prevent any security vulnerabilities
    - report the replacement of a device used for work-related activities immediately to the Committee Chairperson, if the data on the phone was not wiped in its entirety
    - report the loss, theft or replacement of a device used for work-related activities immediately to the Committee Chairperson
    - not use public cloud-based sharing or public back-up services to store business-related personal data without prior authorisation from the Committee Chairperson
    - wipe any setting data from personal devices prior to disposal or passing the device on
    - not retain personal data for longer than is necessary for the purpose for which it is being used, unless there is a requirement to retain it for longer to comply with any legal obligation; if an employee is in any doubt, he/she should contact their Committee Chairperson

- ensure that if family or friends use the affected devices, they are unable to gain access to any personal information that is work-related by, for example, by password-protection
- ensure that if family or friends use the device, they do not install applications, or disable any protective software, contrary to the policy above

- If individuals require any technical support with their device, they should ensure that the third party providing such support has access to any data insofar as is necessary to complete his/her work, and that data is not transferred to a third-party device unless there is no other way of rectifying the technical problem. If data is transferred to a third-party device, the third party must warrant, and the individual must ensure, that the information is removed permanently from such a third-party device once the problem has been rectified.
- Individuals must ensure that if they delete information, it is deleted permanently rather than left in the device's waste-management system. Overwriting software may be needed to achieve this. However, this is not always practicable because, for example, the information is stored or categorised with other information that is still live. In these circumstances, it is sufficient for the individual to put the information 'beyond use', by:
  - ensuring that he/she does not use the personal information to make any decision that affects an individual or in a manner that affects an individual in any way
  - not giving any other organisation access to the personal data in any way
  - surrounding the personal data with appropriate technical and organisational security
  - committing to the permanent deletion of the information if and when this becomes possible
- If an employee uses removable media, for example a USB drive, to transfer personal data, he/she must ensure that the personal data is deleted once the transfer is complete. All removable media used to hold personal data must be encrypted/password protected.
- If an individual leaves the organisation, he/she must delete all work-related personal data on his/her own device prior to his/her last day with the organisation.
- If there has been a breach of personal data, staff/volunteers/trustees must inform Windmills' Designated Person for Safeguarding and Child Protection and the Business Manager as Data Compliance Lead immediately, and change their password/pass code.

Mobile Phones

Please see our separate policy on Mobile Phones and Photographic Images.

Electronic Learning Journals

- Windmills uses a cloud-based electronic learning journal called Tapestry. Staff use the same guidelines for making entries on Tapestry as laid out in the Children's Records Policy, Mobile Phone and Photographic Images Policy, as well as this policy.

- Staff must set a strong password to login to Tapestry and they must ensure their password to Tapestry is kept confidential. If there has been a breach of the password, staff must inform Windmills' Designated Person for Safeguarding and Child Protection and the Data Protection Lead immediately and change their password.
- If staff are accessing Tapestry from home or on a portable device, they must never allow the device to save their password.
- When stepping away from the computer staff must log-out of Tapestry to ensure no one else can access the information.
- Staff are aware that it is an offence to distribute indecent images. In the event of a concern that a colleague or other person is behaving inappropriately, the Safeguarding Children and Child Protection Policy, in relation to allegations against staff and/or responding to suspicions of abuse, is followed.
- Staff are aware that grooming children and young people online is an offence in its own right and concerns about a colleague's or others' behaviour must be reported (as above).

Online productivity tools and cloud-based storage

- To manage our setting efficiently and cost effectively we use 'GSuite', cloud-based productivity and collaboration tools developed by Google for 'Not For Profit' organisations.
- We manage emails through 'Gmail', diary events through 'Calendar', contact information through 'Contacts', and documents ('Docs', 'Sheets', 'Slides') which require collaboration and internal sharing within Windmills via 'Drive'.
- Google outline their compliance with the GDPR in their Privacy Policy https://policies.google.com/privacy and Terms of Service https://policies.google.com/terms

Social Media and Social Networking – Staff & Management Committee

The internet is a fast-moving technology and it is impossible to cover all circumstances. However, the principles set out in this policy should be followed in line with our Staff Code of Conduct and Management Committee Code of Conduct.

Social networking and social media are on-line networks which allow the sharing of information. This is usually information about oneself. This information is invariably targeted at people who are known to an individual such as friends and family; people who don't know you but share common interests, such as other preschool assistants; and anyone who may stumble across you searching on the internet. Social media and social networking sites are very varied and include, but are not limited to - Facebook, Instagram, You Tube, Twitter, LinkedIn, Snapchat, Reddit, Myspace.

Windmills respects everyone's right to a private life and these guidelines are not about stopping the use or access of social media or social networking. However, Windmills must also ensure it does not harm the interests or confidentiality of the children, young people, vulnerable adults, parents/carers, and employees in our care, and that the reputation of the preschool is protected.

The following guidelines are to assist staff and Management Committee members in setting clear expectations of behaviour, support safer working practices and minimising the risk of misplaced or malicious allegations made against staff. These guidelines apply to all staff, volunteers and Management Committee members whether paid or unpaid.

Staff and volunteers **should not**:

- accept parents or other service users (e.g. grandparents/childminders) to view their page on social networking sites, or accept them as 'friends' online. If staff do not already have an online relationship with a parent or service user before their child starts at Windmills this should remain so until after the child and subsequent siblings leaves Windmills. If staff were already friends with parents before becoming service users, then this relationship must remain professional at all times and staff must adhere to the Confidentiality Policy and Staff Code of Conduct;
- disclose personal data or information, without consent, about any individual that could breach the data protection act 1998, which is a criminal offence. Any information regarding the children, their families, other service users or staff, must be kept confidential if learned through the preschool;
- discuss any issues relating to the work place;
- post, or reply to, any comments about the preschool, the children, families, service users, staff or the workings of the preschool on social media;
- share information that they would not want children, parents, service users or colleagues to view;
- conduct themselves in a way that is detrimental to Windmills or could bring Windmills into disrepute;
- allow interaction on websites to damage relationships between members of staff and families of the preschool, or cause offence.
- post any information that breaches copyright
- post material that is abusive, defamatory, sexist, racist, or which could be interpreted as harassment or bullying. Anyone who makes a defamatory statement that is published on the internet may be legally liable for any damage to the reputation of the individual concerned;
- post photos on the internet that link them to Windmills; this includes photos of any of the children or their families, unless permission has been obtained by those concerned. Photos should not be included of staff members in uniform (except on the preschool website with prior permission).

- include hyperlinks to Windmills website from personal websites, blogs or posts.
- make comments on behalf of Windmills or claim to represent the views of Windmills, unless receiving explicit permission to do so.
- make allegations about other employees, or individuals connected with Windmills, another organisation, or the local authority. Doing so may result in disciplinary action being taken. If there are concerns about practices within the preschool or the actions of parents or staff, they must be reported in accordance with our Whistleblowing policy.

It may be deemed a disciplinary offence if any employee is found to be contravening these guidelines. Management Committee members may also lose their position on the Committee.

Committee Members **should not**:

- disclose personal data or information, without consent, about any individual that could breach the data protection act 1998, which is a criminal offence. Any information regarding the children, their families, other service users or staff, must be kept confidential if learned through the preschool;
- share information that they would not want children, parents, service users or colleagues to view;
- conduct themselves in a way that is detrimental to Windmills or could bring Windmills into disrepute;
- allow interaction on websites to damage relationships between members of staff and families of the preschool, or cause offense.
- post any information that breaches copyright
- include hyperlinks to Windmills website from personal websites, blogs or posts.
- make comments on behalf of Windmills or claim to represent the views of Windmills, unless receiving explicit permission to do so.
- make allegations about employees, or individuals connected with Windmills, another organisation, or the local authority. If there are concerns about practices within the preschool or the actions of parents or staff, they must be reported in accordance with our Whistleblowing policy.

Staff, Volunteers, Management Committee members **should**:

- manage personal security settings to ensure that information is only available to people chosen to share information with.
- use their discretion when filling out public profiles which ask for 'place of work' – this applies to staff/volunteers only.
- in the event that Windmills is named in any social media, ensure it is done so in a way that is not detrimental to Windmills, staff, young people, vulnerable adults, children, families, or service users.

- review their social networking sites when they join, and periodically, to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and/or the preschool if they were to be published outside the site.
- report to the Chairperson or Business Manager anything that is posted which gives rise to concerns within this policy, or any other policy.
- be aware of the dangers of putting personal information, such as email addresses and telephone numbers, on sites. This will avoid the potential for families having access to staff and Committee Members outside of the preschool environment.

- The above 'should's' and 'should not's' forms part of our Induction for new employees, volunteers and Management Committee Members.

Before posting on social media staff and committee should ask themselves the following questions:

- Do you want the whole world to see?
- Do you want the post to be seen forever?
- What if the information is taken out of context?
- Could the information put you or others in danger?
- Are you violating any laws?
- Is your message clear?
- Could the actions of your social networking friends reflect negatively on you or Windmills?

Social Media & Social Networking – Parents

- Photos put on the internet by parents should predominately feature their own child and should not include a child's name or be tagged. Parents/carers should also be mindful of the context of the photograph, i.e. does the photo show a member of staff in uniform, is a child getting dressed in the background? If so it should not be posted on the internet.
- Parents are not to use social media platforms to make complaints about Windmills or its staff. If you have a complaint about anything to do with the staff or the preschool, please use our existing formal complaints procedure.
- Parents/carers are respectfully asked not to contact staff via social media to invite them to view their social media profiles or to 'friend' them. Staff are obliged to decline these requests until the family's youngest child leaves the pre-school. This is to protect staff from unwanted misplaced or malicious allegations made against them. Staff should not be put in the uncomfortable position of having to decline. If a parent/carer was already 'friends' with a member of staff before your child started at Windmills, they must be aware that staff must remain professional at all times and will need to use their discretion as to what is acceptable, and when is acceptable, to comment on posts.

- Parents/carers are not to talk about staff on social media, or the methods that are used to look after or educate children. If parents/carers are uncomfortable about the way a situation has been handled by a member of staff, they should speak to them directly. If they are still not happy with the situation, they should use our formal complaints procedure.
- If it comes to Windmills' attention that parents/carers are posting comments that are derogatory or defamatory towards staff, volunteers or committee members, *they will be given a letter in the first instance. If comments persist this may ultimately result in the provision of a child's place being withdrawn.*
- We ask parents to please refrain from setting up Windmills-related 'Facebook' pages or other social networking groups. We aid communication with parents/carers at the preschool by emailing out a termly Contact List to all parents and have good communication processes already in place.

Cyber Bullying

Windmills are committed to ensuring that all its employees are treated with dignity and respect at work. Bullying and harassment of any kind will not be tolerated in the workplace. Cyber-bullying methods include using text messages, mobile phone calls, instant messenger services, by circulating photos or video clips or by posting comments on websites, blogs or in chat rooms. Personal blogs that refer to colleagues without their consent is also unacceptable. Employees who cyber-bully a colleague could also face criminal prosecution under various laws, including the Malicious Communications Act 1988.

Legal framework

- General Data Protection Regulation (GDPR) (2018)
- Equalities Act (2006)
- Malicious Communications Act (1988)