Online Safety Policy
Social media, online communication, Personal and Mobile Devices

January 2018

1. Creating an Online Safety Ethos

- Pipkins Nursery School Chevening believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.
- Pipkins Nursery School Chevening identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.
- Pipkins Nursery School Chevening has a duty to provide the community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.
- Pipkins Nursery School Chevening identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.
- The purpose of Pipkins Nursery School Chevening online safety policy is to:
    - Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that Pipkins Nursery School Chevening is a safe and secure environment.
    - Safeguard and protect all members of Pipkins Nursery School Chevening.
    - Raise awareness with all members of Pipkins Nursery School Chevening regarding the potential risks as well as benefits of technology.
    - To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
    - Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the setting as well as children and parents/carers.
- This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptop, tablets or mobile phones.
- This policy must be read in conjunction with other relevant setting policies including (but not limited to) safeguarding and child protection, behaviour, confidentiality, image use Policies.

2. Online Communication and Safer Use of Technology

2.1 Managing the school/setting website

- The school will ensure that information posted on the Setting website meets the requirements as identified by the Department for Education (DfE).
- The contact details on the website will be the setting address, email and telephone number. Staff or pupils' personal information will not be published.
- The head owner will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
- The website will comply with the setting's guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright.
- Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT'.)
- The administrator account for the school website will be safeguarded with an appropriately strong password.
- The setting will post information about safeguarding, including online safety, on the school website for members of the community.

2.2 Publishing images and videos online

- The setting will ensure that all images and videos shared online are used in accordance with the setting image use policy.
- The setting will ensure that all use of images and videos take place in accordance other policies and procedures including data security, Acceptable Use Policies, Codes of Conduct, social media, use of personal devices and mobile phones etc.
- In line with the image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

2.3 Managing email

- Manager is provided with a specific setting email address to use for any official communication.
- **The use of personal email addresses by staff for any official setting business is not permitted.**
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email.
- Access to setting email systems will always take place in accordance to data protection legislation and in line with other appropriate setting policies e.g. confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the setting safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted. Access in school to external personal email accounts may be blocked.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on setting headed paper would be.

2.4 Appropriate and safe use of the internet and any associated devices

- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole setting curriculum.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of children will be appropriate to their age and ability
    - At Early Years Foundation Stage access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials which supports the learning outcomes planned for the children's age and ability.
- All setting owned devices will be used in accordance with the setting Acceptable Use Policy and with appropriate safety and security measure in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the setting or recommending for use at home.
- Children will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The setting will use age appropriate search tools as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.
- The setting will ensure that the use of Internet-derived materials by staff and children complies with copyright law and acknowledge the source of information.

3. Social Media Policy

3.1 General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of Pipkins Nursery School Chevening and exist in order to safeguard both the setting and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multi-player online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- All members of Pipkins Nursery School Chevening will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of Pipkins Nursery School Chevening.
- All members of Pipkins Nursery School Chevening are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The setting will control staff access to social media and social networking sites whilst on site and when using setting provided devices and systems
- The use of social networking applications during setting hours for personal use is not permitted,
- Inappropriate or excessive use of social media during work hours or whilst using setting devices may result in disciplinary or legal action and/or removal of Internet facilities.
- Any concerns regarding the online conduct of any member of Pipkins Nursery School Chevening on social media sites should be reported to the leadership team and will be managed in accordance with policies such as allegations against staff, behaviour and safeguarding/child protection.

- Any breaches of school/setting policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with relevant policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

3.2 Official use of social media

- Pipkins Nursery School Chevening official social media channels is: www.facebook.com/pipkinsnurseries
- Official use of social media sites by the setting will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the owner.
- Official setting social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- Staff will use setting provided email addresses to register for and manage any official approved social media channels.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use will be in line with existing policies including anti-bullying and child protection.
- Images or videos of children will only be shared on official social media sites/channels in accordance with the image use policy.
- Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.
- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the /setting website and take place with written approval from the Leadership Team.
- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence.
- Parents/Carers will be informed of any official social media use, along with expectations for safe use and l action taken to safeguard the community.

3.3 Staff personal use of social media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the setting Acceptable Use Policy.
- All members of staff are advised not to communicate with or add as ‘friends’ any current or past children or current or past children’s family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead.
- All communication between staff and members of the setting community will take place via official approved communication channels

- Staff will not use personal social media accounts to make contact with parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the manager.
- Any communication from parents received on personal social media accounts will be reported to the setting designated safeguarding lead.
- Information and content that staff members have access to as part of their employment, including photos and personal information about children and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with setting policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.
- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
- Members of staff will notify the Leadership/Management Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the setting.
- **Members of staff are encouraged not to identify themselves as employees of Pipkins Nursery School Chevening on their personal social networking accounts. This is to prevent information on these sites from being linked with the setting and also to safeguard the privacy of staff members and the wider community.**
- Members of staff will ensure that they do not represent their personal views as that of the setting on social media.
- Setting email addresses will not be used for setting up personal social media accounts.
- Members of staff who follow/like the settings social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

3.4 Staff official use of social media

- If members of staff are participating in online activity as part of their capacity as an employee of the setting, then they are requested to be professional at all times and to be aware that they are an ambassador for the setting.
- Staff using social media officially will disclose their official role/position but always make it clear that they do not necessarily speak on behalf of the setting.
- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff must ensure that any image posted on any official social media channel have appropriate written parental consent.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the setting unless they are authorised to do so.
- Staff using social media officially will inform the manager, the Designated Safeguarding Lead and/or the owner of any concerns such as criticism or inappropriate content posted online.

- Staff will not engage with any direct or private messaging with parents/carers through social media and will communicate via official communication channels.
- Staff using social media officially will sign the setting social media Acceptable Use Policy.

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding personal devices and mobile phones

- The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of Pipkins Nursery School Chevening to take steps to ensure that mobile phones and personal devices are used responsibly.
- The use of mobile phones and other personal devices by young people and adults will be decided by the setting and is covered in appropriate policies including the setting Acceptable Use or Mobile Phone Policy
- Pipkins Nursery School Chevening recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within settings.

4.2 Expectations for safe use of personal devices and mobile phones

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate setting policies.
- Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The setting accepts no responsibility for the loss, theft or damage of such items. Nor will the setting accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in certain areas within the setting site such as changing rooms, toilets and nappy changing area.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the discipline/behaviour policy.
- Members of staff will be issued with a work phone number and email address where contact with parents/carers is required.
- All members of Pipkins Nursery School Chevening will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of Pipkins Nursery School Chevening will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.
- All members of Pipkins Nursery School Chevening will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the settings policies.
- Setting mobile phones and devices must always be used in accordance with the Acceptable Use Policy and any other relevant policies.
- Setting mobile phones and devices used for communication with parents and authorities must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

4.3 Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting parents/carer within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with managers.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
- Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures e.g. confidentiality, data security, Acceptable Use etc.
- Staff personal mobile phones and devices will be switched to 'silent' mode during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the /setting policy, then disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, then the police will be contacted.
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the settings allegations management policy.

4.6 Visitors use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the school/settings acceptable use policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.
- The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

5. Policy Decisions

5.1. Reducing online risks

- Pipkins Nursery School Chevening is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.
- The school will ensure that appropriate filtering and monitoring systems are in place to prevent staff from accessing unsuitable or illegal content.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a setting computer or device.

- The setting will audit technology use to establish if the online safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the setting's leadership team.