IT Acceptable Use Policy

Pippa Pop-ins Nursery Schools

Pippa Pop-ins 165 New King's Road (Ofsted ID: EY449873)

Pippa Pop-ins 233 New King's Road (Ofsted ID: EY449869)

Pippa Pop-ins 430 Fulham Road (Ofsted ID: EY449872)

Pippa Pop-ins 5 Kensington Palace (Ofsted ID: EY489562)

Pippa Pop-ins 91-93 Princedale Road (Ofsted ID: 2857426)

Primary person responsible for the implementation and monitoring of this policy:	Ben Murray, Nazish Usman, Joanne Allen
Adopted:	June 2026
Last review:	April 2026
Next review due:	April 2027

Pippa Pop-ins®
Nursery Schools

Contents

1. Scope and Application

1.1 This policy applies to:
Pippa Pop-ins 165 New King's Road (Ofsted ID: EY449873) ("**Pippa Pop-ins**")
Pippa Pop-ins 233 New King's Road (Ofsted ID: EY449869) ("**Pippa Pop-ins**")
Pippa Pop-ins 430 Fulham Road (Ofsted ID: EY449872) ("**Pippa Pop-ins**")
Pippa Pop-ins 5 Kensington Palace (Ofsted ID: EY489562) ("**Pippa Pop-ins**")
Pippa Pop-ins 91-93 Princedale Road (Ofsted ID: 2857426) ("**Pippa Pop-ins**")

1.2 This policy applies to all members of Pippa Pop-ins' community, including employees, including directors, apprentices, casual workers, whether on permanent or temporary contracts (collectively '**staff**') and children who may use Pippa Pop-ins' IT systems as a condition of access. Access to nursery systems is not intended to confer any status of employment on any contractors.

2. Policy Aims

2.1 This policy aims to clarify the following principles that apply to all Pippa Pop-ins staff:

2.1.1 Pippa Pop-ins cannot guarantee the confidentiality of content created, shared and exchanged via nursery systems. Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.

2.1.2 Staff should not access, create or share content that is illegal, deceptive, or likely to offend or misinform other members of Pippa Pop-ins' community (for example, content that is obscene, or promotes violence, discrimination, conspiracy theories or extremism, or raises safeguarding issues).

2.1.3 Staff must respect the privacy of others. Do not share photos, videos, contact details, or other information about members of Pippa Pop-ins' community, even if the content is not shared publicly, without going through official channels and obtaining permission.

2.1.4 Staff must not access or share material that infringes copyright, and do not claim the work of others as your own.

2.1.5 Staff should not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.

2.1.6 Staff should not use their personal email, or social media accounts to contact children or parents, and children and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

3. Using Pippa Pop-ins' IT systems

3.1 Whenever you use Pippa Pop-ins' IT systems (including by connecting your own device to the network) you should follow these principles:

3.1.1 Only access nursery IT systems using your own username and password. Do not share your username or password with anyone else.

3.1.2 Do not attempt by any means (including by the use of a Virtual Private Network (VPN)) to circumvent the content filters or other security measures installed on the IT systems, and do not attempt to access parts of the system that you do not have permission to access.

3.1.3 Do not attempt to install software on, or otherwise alter, nursery IT systems.

3.1.4 Do not use the nursery's IT systems in a way that breaches the principles of online behaviour set out above.

3.1.5 Remember that Pippa Pop-ins monitors use of its IT systems, and that Pippa Pop-ins can view content accessed or sent via its systems.

3.2 The provision of nursery email accounts, Wi-Fi and internet access is for official Pippa Pop-ins business, administration and education. Staff and children should keep their personal, family and social lives separate from their nursery IT use and limit as far as possible any personal use of these accounts. Again, please be aware of Pippa Pop-ins' right to monitor and access web history and email use.

4. Passwords

4.1 Passwords protect Pippa Pop-ins' network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

5. Use of Property

5.1 Any property belonging to Pippa Pop-ins should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the Head of the Nursery.

6. Use of Personal Devices or Accounts and Working Remotely

6.1 All official nursery business of staff must be conducted on Pippa Pop-ins systems, and it is not permissible to use personal email accounts for nursery business. Any use of personal devices for work purposes, and any removal of personal data or confidential information from Pippa Pop-ins systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by IT Manager Ronak Mehta.

6.2 All staff must recognise that once something is posted online it has a persistence that is not like something that is said. It is also replicable and searchable (directly and through its metadata), and you cannot be sure who your audience is or will be. Once something is posted online, its effects are often magnified and can be mirrored out of context. For example, hashtags can link your content to other content with the same hashtag; retweeting a post can be viewed as a public sign of endorsement, which may be inappropriate in some circumstances. All of this requires experience to understand. Remember: when you post, you have not only your own reputation to consider but also that of others and that of Pippa Pop-ins. Every member of the

community has to take responsibility for his or her actions online. If you are in doubt, it is best not to post, send an email, etc. We encourage staff to use digital technologies but to do so in an informed, thoughtful way that is fully consistent with the position of trust we occupy.

6.3 Staff should ensure that they understand the tools they are using, the implications of any privacy and sharing settings, and, on a site-by-site basis, the terms and parameters of any connections or networks made. Staff should ensure their settings prohibit others from tagging them in any photos or updates without their permission and be proactive in asking others to remove any undesirable content related to them. Social media sites often update their privacy settings and may add new features. Staff are advised to revisit their privacy settings on a regular basis to ensure they remain effective. When joining or being added to a Facebook (or other social media) group, always check whether it is public, closed (where anyone can see the members of the group but not the discussion) or secret (where neither the members or the discussion are visible). Staff who use social media sites should ensure maximum privacy settings are used.

6.4 Particular awareness is necessary of issues associated with the words deployed to describe the establishment of contacts and networks on-line: there are innumerable ways, across countless sites, of defining or describing contacts and connections. For example, Facebook has distorted the usual understanding of the term “friending”, and there are “circles” on Google.

6.5 In any professional capacity, staff must not use pseudonyms or post anonymously, though it is good practice to signal any Pippa Pop-ins-related account as being distinct from a personal account (by using your title and surname, or role or designation). Staff must ensure they do not claim or appear to claim to represent or speak in the name of Pippa Pop-ins except where specific permission to do so has been given by the Head of Nursery. A Pippa Pop-ins email address should never be used for any personal use of social media.

6.6 Staff may, of course, choose to use social sites and apps in a personal capacity. It remains the case that ‘when you post, you have not only your own reputation to consider but also that of others and that of Pippa Pop-ins. You may wish to say where you work and what you do. Many people who do this include a disclaimer along the lines of, 'the views expressed here are my own and not my employer’s'. Such a disclaimer in no way dispenses with the need to exercise good judgement and care in what you say and do online.

6.7 All staff must understand the standards of behaviour expected of them. Breaches of these standards may result in disciplinary action. Such breaches might include, but are not restricted to:

6.7.1 failure to comply with the law or relevant regulatory bodies;

6.7.2 communication of confidential or personal information;

6.7.3 defamation or disparagement of Pippa Pop-ins and its staff;

6.7.4 harassment or bullying; and/or

6.7.5 failure to comply with our policy concerning the use and distribution of images.

6.8 Under no circumstances should adults in Pippa Pop-ins access, or attempt to access, inappropriate images, videos, media or materials. Accessing child pornography or indecent

images of children on the internet, and making, storing, or disseminating such material, is illegal and, if proven, will lead to the individual being barred from working with children and young people.

6.9 While members of staff are provided with a Pippa Pop-ins email account for professional use, it is recommended that they also have a separate account with the provider of their choice for personal email communications. During the nursery day our primary focus should be the education and welfare of children and any personal correspondence or business should not substantively inhibit or conflict with that focus.

6.10 In all things, staff should act with consideration and with an awareness of the trust invested in them for the safeguarding of children. Moreover, staff should be proactive in promoting good online practice by every member of the community. Your judgement will be informed by your experience, prior training, character, and the context of any given situation, but it must also be informed by your professional obligations. Should you receive any abusive messages, it is advisable not to delete them but to keep a record of them to facilitate any subsequent investigation.

7. Monitoring and Access

7.1 Staff, parents and children should be aware that nursery email and internet usage (including through the nursery Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and nurser email accounts may be accessed by Pippa Pop-ins where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

7.2 Pippa Pop-ins may require staff to conduct searches of their personal accounts or devices if they were used for nursery business in contravention of this policy, and in particular if there is any reason to suspect illegal activity or any risk to the wellbeing of any person.

8. Tracking Devices and Technology

8.1 While the Pippa Pop-ins is not responsible for individual settings on personal devices, our general position is that tracking technology that relies on location data sourced from third party devices should not be used on nursery premises or on trips – given the potential privacy concerns for third parties.

8.2 That said, Pippa Pop-ins is aware that there may be instances where such technology – whether, for example, for security of belongings or for parents' peace of mind as to children's whereabouts – can be used appropriately and proportionately. We would encourage parents to raise any such requests with us, for example in advance of a trip, so that we can discuss appropriate usage.

9. Compliance with Related Policies

9.1 To the extent they are applicable to you, you will ensure that you comply with Pippa Pop-ins' related policies, including (but not limited to), Safeguarding and Child Protection Policy, Code of Conduct and Data Protection Policy.

10. Retention of Digital Data

10.1 Staff must be aware that all emails sent or received on nursery systems will be kept in archive whether or not deleted and email accounts will generally be closed and the contents deleted/archived within 1 year of that person leaving Pippa Pop-ins.

10.2 Any information from email folders that is necessary for Pippa Pop-ins to keep for longer, including personal information (e.g. for a reason set out in the Privacy Notice), should be held on the relevant personnel or child's file. Important records should not be kept in personal email folders, archives or inboxes, nor in local files. Hence it is the responsibility of each account user to ensure that information is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of Pippa Pop-ins' email deletion protocol.

10.3 If you consider that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact IT Manager Ronak Mehta.

11. Breach Reporting

11.1 The law requires Pippa Pop-ins to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

11.2 This will include almost any loss of, or compromise to, personal data held by Pippa Pop-ins regardless of whether the personal data falls into a third party's hands. This would include:

11.2.1 loss of an unencrypted laptop, USB stick or a physical file containing personal data;

11.2.2 any external hacking of the nursery's systems, e.g. through the use of malware;

11.2.3 application of the wrong privacy settings to online systems;

11.2.4 misdirected post, fax or email;

11.2.5 failing to bcc recipients of a mass email; and

11.2.6 unsecure disposal.

11.3 Pippa Pop-ins must generally report personal data breaches to the ICO without undue delay (i.e. within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, Pippa Pop-ins must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

11.4 If staff become aware of a suspected breach, they must immediately inform the Principal/NI, then they must inform Head of Safeguarding and Head of Health and safety.

11.5 Data breaches will happen to all organisations, but Pippa Pop-ins must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff. Pippa Pop-ins' primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either

by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

12. Breaches of this Policy

12.1 A deliberate breach of this Policy by staff will be dealt with as a disciplinary matter using Pippa Pop-ins' usual applicable procedures. In addition, a deliberate breach by any person may result in Pippa Pop-ins restricting that person's access to nursery IT systems.

12.2 If you become aware of a breach of this Policy, or you are concerned that a member of the Pippa Pop-ins community is being harassed or harmed online you should report it to the Principal/NI and must also inform head of safeguarding and compliance and head of health and safety. Reports will be treated in confidence wherever possible.