Friern Barnet School

Acceptable Use Policy for Staff

(ICT Resources)

Last Reviewed:	November 2024	**Next Review:**	November 2026
Approved by:	Head Teacher	**Date:**	29 November 2024

Friern Barnet School
Acceptable Use Policy for staff
(ICT resources)

Rationale

ICT resources in its many forms are vital part of our daily lives. Because of the pace of change, staff are expected to exercise caution when experimenting with new technologies where it may compromise themselves, their colleagues and our students. As some internet material is of an unacceptable nature and may compromise safeguarding, the use of the internet and e-mail within Friern Barnet School may be restricted.

Defining ICT
Staff, governors and visitors understand that ICT includes a wide range of systems, including mobile phones, laptops, tablets and digital cameras.

Aims

The aim of this Acceptable Use Policy is to ensure that staff will benefit from learning opportunities offered by the school's ICT resources in a safe and effective manner. This policy applies to both on site and remote learning.

The school's network is a system of interlinked devices which staff and students use in order to gain access to internal ICT recourses, internet, email facilities and any other technologies for uses permitted by the school. This policy applies to all ICT resources owned and maintained by Friern Barnet School, whether attached to the network or not and any other electronic devices used on site for private use.

Practice

All staff are responsible for ensuring that they do not breach the guidelines listed below:

1 Access is provided for curricular and administrative use and is not generally for private use

2 Staff will only use the school's ICT resources and systems for professional purposes or for uses deemed reasonable by the Head Teacher and Governing Body. All devices issued by the school will be password protected

3 Staff will not browse, download or send material that could be considered offensive, illegal or discriminatory to students, colleagues or anyone outside the organisation

4 Staff will report any accidental access to, or receipt of inappropriate materials, or filtering breaches to the Network Manager

5 Staff will not download any software or resources from the internet that can compromise the network or are not adequately licensed

6 The following are prohibited:

- bypassing filtering or security systems in place
- damage to computers, computer systems or computer networks
- vandalising, damaging or disabling another person's property
- debilitating or disabling computers
- altering setup or settings of computers and software without the express permission of the Network Manager

7 Staff will ensure that they do not violate copyright or intellectual property. Any materials including, music, videos/films and print resources sourced should be used in compliance with The Copyright and Related Rights Regulations 2003 and Copyright, Designs and Patents Act 1988 (always give credit to the person or company that owns the materials)

8 Any access to the internet for private use must be carried out within the member of staff's free time. (Staff should be aware that all internet usage and network usage is logged.)

9 No staff, governors or visitors will disclose or share login details provided to them by the school. Passwords must not be written on paper or recorded in a way that it can be used by someone else

10 Staff will ensure that any document with personal data is password protected and only shared with relevant individuals. Staff must protect any school data by not leaving their device open, either in school or at home

11 Staff will ensure that any private social networking sites/blogs etc that they create or actively contribute to, do not compromise their professional responsibilities within the school. Further they must ensure that they do not engage with students, under the age of 18, through social networking sites and unauthorised blogs, both inside and out of school. Staff should recognise that Facebook and many social networking services (SNS) do have a minimum age requirement of 13. **Please refer to Appendix B of this policy**

12 Staff must not setup social media accounts on any platform to represent the school

13 Staff will not engage in any online activity that might compromise their professional responsibilities

14 Staff should be aware of digital safe-guarding issues and should embed these into their classroom practice

15 Staff will only use the approved, secure email system for school business. Staff should not open unexpected emails but should report these to the Network Manager

16 Any electronic communication that contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using the LGFL encrypted email system

17 Staff must not send e-mails or attachments that could cause offence through content that is for example, racist or sexually explicit. Staff must not use email in ways that might constitute harassment of others (whether or not they are the recipient of messages) by containing content or language that is abusive, offensive, or derogatory, or by unreasonably persistent e-mailing of groups or individuals

18 Remote learning will take place using Microsoft Teams and Firefly

19 Use of any personal accounts to communicate with learners and parents/carers is not permitted. Staff will only use school managed email and login accounts for remote learning

20 Remote teaching sessions must be recorded using Microsoft Teams. All participants will be made aware that the session is being recorded

21 Online contact with learners will only take place in normal school time

22 Photos and videos of students must, where possible, only be taken using the school owned devices. Where staff use their personal device for capturing images / videos during school trips and events, they must ensure that these are transferred on to the school's network and deleted from their personal device at the earliest possible opportunity

23 Staff choosing to connect their personal devices to the school's wireless network, accept that they must comply with the requirements and terms set out in this policy

24 Staff must not use any device other than the school PCs, or portable devices such as laptops, phones and tablets issued by the school when handling personal data

25 If you use mobile device(s) to access school email you must make sure that they are protected with a password or pass-code logon. If the device is lost or stolen, you must inform the Data Protection Officer as soon as possible so that the information stored on the device can be remotely wiped off

26 Staff must not store/transfer personal data on USB sticks and other portable storage devices other than those issued and encrypted by the school IT department. The USB drive should remain physically secure both in transit and when stored on site. It must not be taken out of the EU. Should this USB drive go missing, you must inform the DPO or Network Manager immediately. When your employment with the school terminates, you should return the USB drive to the Network Manager for secure disposal. Data must not be copied from the encrypted USB drive onto any personal computer equipment used off site (this includes home computers). In general there should be no need to store data outside school

27 Artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Friern Barnet School recognises that AI has many uses to help students learn, but also poses risks to sensitive and personal data. To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Friern Barnet School will treat this as a data breach, and will follow the personal data breach procedure outlined in Appendix 1 of the Data Protection Policy.

28 Any information seen by staff with regard to other members of staff or pupil information held within the school's management information system, will be kept private and confidential, *except* when it is deemed necessary by law to disclose such information to an appropriate authority

29 Ensure that data is not visible to students or other unauthorised personnel. This includes any data in SIMS

30 Upon termination of employment staff must not attempt to copy files from any shared drive or personal area to their own personal external drives. This data remains the property of Friern Barnet School

31 Staff must read Appendix A of this policy, sign and return it to their line manager

32 Failure to comply with this Acceptable Use Policy could lead to disciplinary action

General Advice to Users:

1 Notify the Network Manager immediately if by accident you encounter materials that violate this Acceptable Use Policy.

2 Ensure you do not log students onto the computer system with your own passwords.

3 Ensure that your passwords for access to the network, email, Firefly and SIMS are strong passwords. You should change these on a regular basis, and not tell other members of staff or students your passwords.

4 Ensure that you lock or log out your computer when leaving it unattended, even for a short period of time. You are responsible for activity that takes places using your credentials.

5 When you leave the school, be aware that your accounts for the network, email and other systems will be disabled when your contract ends.

6 Files should be deleted from the network and encrypted USB drives when no longer needed, in line with the school's data retention policy. When deleting a file from a USB drive outside of school you should use shift and delete to avoid the risk of a copy of the file being stored in the recycle bin.

Using social networking services (SNS) Appendix B

Many teachers and professionals use social networking services (SNS), such as Facebook and Twitter, in order to stay in touch with friends and family. This guide is designed to support your personal use of these services, keeping you, your students, and your job safe.

Do not accept requests to follow you from pupils, recent pupils or even parents at your school. On most services, the sender won't be notified if you select ignore/not now or delete for such requests, nor, if you had already accepted such a request, will they be notified if you remove them from your friends list or followers. By accepting such requests you could be making yourself vulnerable by sharing personal information or by having access to personal information about your pupils. You may be potentially leaving yourself open to allegations of inappropriate contact or conduct or even find yourself exposed to unwanted contact.

Friern Barnet School uses SNS to connect and communicate with pupils, parents, and governors, using our organisational accounts, whilst recognising that many SNS do have a minimum age requirement of 13.

It is important that when using SNS you are in control of who can see your account details and content including photos and albums, posts, status updates and any personal information. On Twitter, you can set your account to private by selecting 'Protect my tweets' so you can then accept (or decline) requests to follow you. In the case of Facebook, choosing a basic 'Friends' setting for every option would initially achieve this. However, you are able to customise each option further, and can limit the information that certain individuals see. It is a good idea to use the "view as" option, to check and see how your profile appears to strangers, and that the information you want to remain private or 'friends only' is not visible. If you are unsure about how to use the settings available, treat all information that you post as being public and act accordingly.

Think carefully about whom you are friends with, and which friends can access what information. It is a good idea to remove any "friends" or customise the privacy settings for current friends, if access to your personal activity could compromise your position, for example parents with children at your school. However, whatever setting you use, it's important always to think before you post because 'Friends' settings do not guarantee privacy. Sharing content with others could mean that you lose control of it, if friends pass on your information, for example.

Think carefully about comments you post on friends' walls, if their profile is not set to private your posts will be visible to anyone.

Geolocation services are beginning to be used to support teaching and learning. However, there are obvious issues in making sensitive information public, for example where you are at a given time or the places you regularly visit. When using location services on SNS, think about making your location visible to only your friends and ensure that you are happy with the friends in your list. The option for being 'checked into' a place by someone else can be disabled in your privacy settings, so you can keep control of your location information.

Your professional reputation is clearly valuable to your current and future career and consequentially managing your online reputation is an essential part of being a teacher. Always think carefully before making any posts, status updates or having discussions regarding the school, its staff, pupils or

parents in an online environment - even if your account is private. Comments made public could be taken out of context and could be very damaging. Think about the language you use, abrupt or inappropriate comments, even if they were made in jest, may lead to complaints. Anything that is put online is potentially public and permanent.

Posting derogatory comments about pupils, parents or colleagues is never acceptable. Teachers are required to uphold the reputation of the school, to maintain reasonable standards in their own behaviour, and to uphold public trust in their profession.

Use a strong password and log out of the SNS after using it. Not logging out means the next user of the computer or other access point can access your SNS account. Deleting cookies may be necessary if you had selected the 'remember this password' option when you were logging in. If you access social networking via an application on your mobile phone, it is a good idea to set a PIN or passcode for the phone, and to remember to log out of the SNS app after each session, so if you mislay your phone, access to your SNS account is still protected.

Be mindful of how you present yourself when you are choosing a profile image, or even when joining a Group or 'liking' pages - think about what these choices say about you. Consider making private, or removing, previous online content that might compromise your current position. It is possible to deactivate existing SNS accounts and to permanently delete profiles. It is important to be aware, however, that though such changes will be immediate on the service itself, content which was visible on public search may still be visible on public search results for a week or two (or even longer) until these changes have been recognised by the search engine.

Searching your name regularly on public search engines can be a useful way to monitor your online content or 'digital identity'. Other tools are also available, for example, utilising privacy settings and removing your profile page from a search engine result. Your online reputation is important for your current and future employment - it is common for employers to search prospective employees online.

If you are unhappy with photos in which you are tagged, untag yourself or alternatively contact the friend and ask them to remove this content. Never be shy about asking others to take down or make private content that identifies you that you are not comfortable with. Be thoughtful about content you post that relates to others and respond positively to requests to take down or make content private. If you think that the image or video breaks the SNS's terms of use, report it to the SNS who can take content down (look for the Report Abuse options in the service).

If you are the victim of cyberbullying, for example, a pupil makes inappropriate comments or posts images of you or another member of staff, don't retaliate and save/print all available evidence (wall posts, URLs, messages, comments etc). The school has a statutory duty of care for the health, safety and welfare of school staff and will therefore take reasonable steps to support staff experiencing cyberbullying.

If you come across, or are made aware of, inappropriate use of social networking sites by your pupils (including under age use of these services), you should report these to the Designated Safeguarding Officer.

Adapted from Childnet International

Appendix A

Acceptable Use Policy for Staff

(Internet, intranet and email)

Please complete and return this form to Friern Barnet School.

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Acceptable Use Policy (normally an annual revisit).

I agree to abide by the school's most recent Acceptable Use Policy.

I wish to have an email account; be connected to the Internet; be able to use the school's ICT resources and systems.

Signature …… Date ……

Full Name …….. (print name)

Job title . . . . . .

School: Friern Barnet School

To: Network Manager

I approve this user to be set-up.

Signature …….. Date ……

Authorised Signature (member of Senior Leadership Team)

Full Name ……. (print name)