THE THINKING SCHOOLS FEDERATION

London Borough of Redbridge

Acceptable Use Policy

2024/25

Contents

1 Introduction

This policy has been developed to clearly state the expectations of Highlands primary school in respect of all persons using equipment, facilities and information belonging to the school.

This policy covers the use of:

- Information, with particular reference to personal information,
- Equipment (including but not limited to computers, laptops, tablets, cameras and smartphones as managed by the school),
- Internet and other connected services
- Email and other correspondence and communication channels including social media and other digital and online societal services including WhatsApp

Failure to adhere to the Acceptable Use Policy will result in appropriate disciplinary action in line with the School's Disciplinary procedures for breaching policy. The school requires users to accept that:

- This policy applies no matter your work location i.e., in the school, at home, remotely or mobile working.
- You **are** aware that improper use of any school information can result in either you and/or the school incurring civil or criminal liability, so the school reserves the right to report any illegal activities to the appropriate authorities.

2 General conduct

As a user of the school's information and information systems, you are expected to act in a professional and responsible manner and therefore you **must not**:

- Attempt to make changes to information or information systems where you have no explicit permission or authorisation, or where any change made could be construed as fraudulent or illegal. This includes installing or attempting to reconfigure any software or delegating such a change to another user.
- Make statements on your own behalf or on behalf of the school, using any of the school's communication channels, which are or may be defamatory, bring the school into disrepute or imply that you are acting on behalf of the school when you have no authority to do so.

- Carry out any action to extract, degrade, hinder or deny access to information to you or other authorised users.

- Extract information for any purpose other than school business

- Use school systems to breach or attempt to breach, including accessing information you are not authorised to access or otherwise process, any legislation. These include but are not limited to, Protection of the Children Act; the Obscene Publications Act; the General Data Protection Regulations (UKGDPR 2020); Data Protection Act 2018; Freedom of Information Act; Intellectual Property Legislation; Copyright Legislation; and the Computer Misuse Act.

- Place school information at risk by handling it in an insecure manner within or outside of school premises.

Any of the above may result in the application of the school's Disciplinary processes or notification to the Police or Information Commissioner.

3 Confidentiality

In order to maintain confidentiality

- Do not forward to any internal or external party information that may compromise the rights of a pupil, parent or staff member or third party in relation to their confidentiality

- Where you have received an email in error, notify the sender that you have received the message in error and then delete any copies of misdirected messages. If the email contains sensitive or personal information notify the designated data protection lead (DDPL) that information has been disclosed to you in error.

- Information should only be shared where there is a business need to do so and this should be in accordance with data protection regulations. Sharing of personal-sensitive information or otherwise confidential information should be approved by your line manager.

4 Access control

To ensure only authorised users can access the school information and systems:

- You **must not** use a colleague's username or password or two-factor authenticator (credentials) to gain access to any information or system.

- You **must not** attempt to access any information or system that you have not been given explicit permission to access.

- You **must not** share your credentials or use them to log another person into the network even if you are asked to by your line manager.

- You **must not** re-use credentials or passwords that you use in your personal life for work purposes

- You **must** notify the loss of your credentials or where a third-party gains access to your password, by reporting this to your data protection lead immediately.

- You **must** notify your IT Support to disable your account as soon as you become aware of any unauthorised access using your credentials.

  You **must** lock your computer screen when away from your device using the keyboard locking mechanism to protect on-screen information (Windows – L).

- You **must not** move information assets to personal folders unless authorised

5 Email Usage

Email is an effective business tool for communicating with colleagues, parents, suppliers and partners both inside and outside the school.

Email is **not** a fully secure means of communication. It does not provide immediate or guaranteed delivery.

All emails sent or received using the school's systems are the property of the school. The school maintains the right to disable user access and to review work emails on the basis of exceptional need, for example to investigate a data breach, safeguarding issue or for business need.

All messages will be unpacked and scanned for viruses as they arrive or leave all school systems.

Users of school Email **shall**:

- Send all sensitive information using Egress. This will also indicate to the recipient how you expect them to handle the information

- Take great care **not** to click on unsolicited links that may be malicious and take all directed steps to prevent a ransomware attack

- Double check attachments are for the intended recipient before sending

- Send all emails involving more than one third party, such as parents or providers, by BCC not CC

- BCC should not be used for more than 10 recipients in a single email and school parent communication tools should be used as a preference

- Send confidential or sensitive personal information to general email addresses (e.g. Hotmail, yahoo, gmail, msn) using encrypted email; except when documented consent is given by the data subject

- Ensure emails never contain children's full names either in the subject line and only where necessary in the main body of the text.

- Use "Private" calendar appointments where the subject of meeting indicates confidentiality may be a concern

- Treat email correspondence as a permanent written record which may be read by persons other than the addressee and store these in appropriate network locations in a structured manner according to the retention schedule.

- Review their Email mailbox regularly and delete unnecessary messages

- Treat unsolicited Emails from unknown sources with the upmost suspicion

Users of school Email **shall not**:

- Use language which includes swear words or may be considered offensive, abusive or unprofessional

- Send school information to or from your own personal email address especially where this includes sensitive personal information of a pupil or staff member

- Download school information to non-school or personal devices or cloud storage

- Set up automatic forwarding of email rules to external email accounts

- Send bulk emails without authorisation

- Transmit PIN (personal identify numbers) or PAN (personal account numbers) used in credit card transactions via email or any other messaging systems unless

appropriately encrypted.

- Send outbound email from generic email accounts set up to receive incoming email only or forward “chain” or joke emails to others
- Use school email addresses and other official contact details for setting up personal accounts for websites, services or social media
- Rename email attachments or password protect attachments to evade malicious software scanning
- Seek to gain access to another user’s mailbox without their consent or the written approval of a senior leader
- Avoid long confusing chains emails should be concise and serve a business purpose
- Never send an email with a attachments without first checking it is the correct one

Where you are replying to emails take care to remove personal data from the correspondence chain where appropriate. The onus is on **you** to protect data in transit.

6 General Usage Guidance

6.1 Desktop / Laptop computers

Desktop/Laptop computers **must not** be used to store any data, including personal, sensitive data. Data stored on the device may not be backed up, and are at risk of loss, theft, or damage by viruses or other malicious software such as spyware.

You **must not** store any non-work related (i.e., not for school business) files, personally owned software or pictures on school managed systems or shared folders.

You **must not** store personal data or data that does not originate from school of any form in any format on school devices or storage media.

You **must not** store personal information in paper formats alongside your laptop\device

You **must not** use personal storage devices or cloud services to access or store school information.

It is school policy to monitor electronic file storage usage, and to remove any software or files deemed inappropriate or pose a risk to the school’s information systems, break copyright legislation or are not for work purposes.

6.2 Removable Media

Removeable media such as memory sticks should **not** be used to hold personal data unless approved by a senior leader for a specific and recorded purpose.

All removable media **must** be approved before use on the school's computer systems and network.

If you are in possession of unencrypted portable media holding personal data, please contact IT Support **immediately** to arrange its collection and disposal.

6.3 Personal Use

The school recognises that occasional personal use of the school's computer is beneficial for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use:

- Must comply with all other conditions of this policy as they apply to non-personal use, and all other school policies regarding staff conduct.
- Must not interfere in any way with your other duties or those of any other member of staff.
- Must not have any undue effect on the performance of the computer system; and
- Must not be for any commercial purpose or gain unless explicitly authorised by the school.

Staff may use the school Email system and internet access for personal use, provided such use does not breach the code of conduct. Permitted personal use **must not** impact on your day-to-day work.

Personal use is permitted at the discretion of the school and can be limited or revoked at any time.

- In addition, your personally owned devices **must not** be connected to the school's data network except where this has been expressly authorised.

The school will not be liable for damage to personal items that are connected to its equipment E.g mobile phones being charged through USB ports.

6.4 Software and Downloads

All users are prohibited from installing software and applications onto the network or devices without permission from IT Support.

Copyright and intellectual property rights must be respected when downloading from the internet.

6.5 Images/Videos

Parental consent is required for all children to have photographs or videos published electronically or in a public area even if they are unidentifiable.

6.6 Network Protocol

The network protocol is as follows:

- School computer and Internet use must be appropriate to a pupil's education or to staff professional activity.
- Respect other people's material and do not corrupt, interfere with or destroy it.
- Do not open files containing personal information without express permission.
- When working with personal data ensure that the data is secure and cannot be viewed by unauthorised persons. Personal data must not be entered into AI solutions
- Input information, especially into school communication channels, accurately and only share with relevant parties.

6.7 Internet Usage

- Ensure all Internet access is carried out under your login account only
- Ensure that Internet access is for the purpose of your contractual obligations only
- Pupils must be supervised at all times when using the internet
- Activities should be planned so 'open searching is kept to a minimum. The facility for caching sites should be used prior to using the internet with pupils
- When searching the internet with pupils, adults should encourage the children to use 'child safe' search engines. However safe search is set on all computers in school as a default on search engines
- The use of social networking sites, chat rooms and messaging systems (e.g. Facebook, Instagram, X, WhatsApp) is **not** allowed on school systems

- Use of school network environments for personal financial gain, gambling, political purposes or advertising is forbidden

- Do not attempt to visit websites that may be considered inappropriate or illegal. Downloading some material is illegal and the police or other authorities may be called to investigate

- The school's IT system automatically monitors all internet usage, so you are responsible for all sites accessed under your login as this information is recorded for compliance purposes.

6.8 Social Networking and messaging applications

Staff must take care when using websites such as Instagram, Snapchat, Tik Tok, Facebook, X, and dating sites etc, even when such use occurs in their own time using their own computer at home. These sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children. Messaging applications, such as WhatsApp offer convenience but should never be used for sharing, disseminating or decision making with personal or business information.

You must not allow any pupil to access personal information you post on a social networking site. In particular:

- You must not add a pupil to your account or communicate with one online

- Your privacy settings should ensure that personal information is not accessible

- You should avoid contacting any pupil privately via social networking even for school-related purposes

- You should take steps to ensure that any person contacting you via a social networking is who they claim to be, and not an imposter, before allowing them to access to your personal information

It is advised not to accept invitations from the pupils' parents or careers to join them on their social media nor should you invite them to be your friends. As damage to professional reputations can inadvertently be caused by quite innocent postings or images. You will need to ensure that any private social networking sites/blogs that you create or actively contribute to are not to be confused with your professional role in anyway.

Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.

- Unless authorised to do so, you must not post comments online that may appear as if you are speaking for the school

- You should not post any material online that can be clearly linked to the school that may damage the school's reputation

- You should avoid posting any material clearly identifying yourself, another member of staff, or a pupil, that could potentially be used to embarrass, harass or defame the subject

Encrypted messaging applications such as WhatsApp or Facebook Messenger are not managed by the school. Information stored on them cannot be retrieved should it be required for statutory or legal purposes. Use of pupil data on encrypted messaging services can therefore be considered detrimental to our responsibilities as a data controller

- Do not share personal information via encrypted messaging application of either staff or pupils
- Only use encrypted messaging applications for business as usual activities
- If school information is processed on an encrypted messaging application managed by yourself we may require access to it in the event that is required
- If school information is shared with you by third parties this should be reported to the designated data protection lead and the information moved to school systems if appropriate

6.9 Use of your own Equipment

- Any personal devices or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff and must not be used until approved. This test must be performed at regular intervals as required by school's normal rules on electrical safety testing

- You must not connect personal devices to school systems

6.10 Interactive boards

Care should be taken to ensure that personal data is not shared on classroom interactive monitors or whiteboards. The use of virtual keyboards should be avoided to prevent access to passwords.

6.11 Mobile Devices

No images of the children should be taken without parental consent and permission from a member of staff using any mobile device e.g. phones, school cameras. These devices must

not be removed from the school premises if they contain images of pupils and without permission from a member of staff.

Mobile phones

- Personal mobile phones should not be used in areas of school where pupils have access

- During teaching time, mobile phones should be turned off or put on silent mode and stored in a cupboard or locker away from the children

- Adult are allowed to access their personal phones on breaks, lunch times and after school in designated areas e.g. staff room or teachers room (safe, suitable places where the children are not present)

- It is forbidden to take photographs/videos of the children on personal mobile phones

Digital cameras and devices with built in cameras

The school encourages the use of digital cameras, video equipment and tablets; however, staff should be aware of the following guidelines:

- Photos should only be named with the pupil's name if they are to be accessible in school only. Photos for the website or press must only include the child's first name

- The use of personal cameras in school is not permitted, including those which are integrated into mobile phones

- All photos should be downloaded to the school network

6.12 Supervision of Pupil Use

- Pupils must be supervised at all times when using school computer equipment.
- Supervising staff are responsible for ensuring that the separate Acceptable Use Policy for pupils is enforced.
- Supervising staff must ensure they have read and understand the separate guidelines on e-safety

6.13 Reporting IT issues and events

It is the job of the IT Manager to ensure that all school computer systems are working optimally at all times and that any faults are rectified as soon as possible.

- You should report any problems that need attention to IT Support via the servicedesk

- If you suspect your computer has been affected by a virus, phishing email or other malware you must report this to IT Support **immediately**

- If you have lost documents or files you should report this as soon as possible. The longer a data loss problem goes unreported, the less chance of it being recoverable

6.14 Reporting Breaches of this Policy

All members of staff have a duty to ensure this Acceptable Use Policy is followed. You must immediately inform the data protection lead or the Head Teacher, of abuse of any part of the networked system. In particular, you should report:

- Any websites accessible from within school that you feel are unsuitable for staff or pupil consumption

- Any inappropriate content suspected to be stored on networked systems.

- Any breaches, or attempted breaches, of personal information, access privilege or security

- Any instance of bullying or harassment suffered by you, another member of staff, or a pupil via school systems.

All reports will be treated confidentially but all of the above could result in appropriate disciplinary action in line with the School's Disciplinary procedures for breach of policy.

6.15 Electronic Devices - Searching & Deletion

In accordance with 'The Education Act 2012' a school has the right to search and or delete anything from personal devices if they believe illegal or suspicious activity is taken place.

7 Remote Working

Remote or mobile working requires a higher degree of care as the risk to information is greater. You should familiarise yourself with the following:

Devices must be completely shut down during transport to ensure that the encryption is enabled. School information including pupil work should not be left in a car for more than 10 minutes and never over night.
Paper pupil\staff records should not be carried in laptop bags to reduce risk in case of theft.

Ensure your devices are password secured if you leave them for a short period by locking the screen, even when you are working at home so no one else can view school information.
Always use strong passwords and do not use passwords you use personally for work devices, even at home.
Only hold confidential calls in private areas.
You must make a record of what personal sensitive data you are taking out of the office in paper format and which senior leader gave authorisation. This means that we can quickly and accurately assess the risk if the papers are lost or stolen.
When working from home, paper records must be kept secure when not being used and must be returned to the office and disposed of as appropriate.
Take great care when using email to avoid clicking on links that may be malicious

8 Lost or stolen

If school information is lost or stolen in the UK or abroad, due to a burglary or street robbery, you **must** report this to IT Support so that it is logged as lost or stolen.

The Designated Data Protection Lead **must** be notified immediately of losses if data stored on the device is of a personal, or personal sensitive nature. This is because the school is required by law to report a breach in under 72 hours if risk criteria are met.

9 Return of school assets

All users, issued with computer equipment **must** return all assets upon termination of their employment, contract or agreement. This includes any removable storage media, laptops, mobile phones, tablets, software, computers, printers and any other computer equipment for home or mobile working.

Managers shall ensure that their staff return all equipment as part of the exit procedures, and notify IT so that their accounts are closed. All equipment shall be returned to IT for reallocation.

10 Review and evaluation

This policy is reviewed annually and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff. Our Acceptable Use Policy (AUP) has been created by our school governors and senior managers in conjunction with the London Borough of Redbridge and approved by the whole school community.

I will adhere with this policy and I *understand that if I become aware of a data breach or the potential for a data breach caused either by myself or by another individual, I MUST inform the Headteacher or Designated Data Protection Lead immediately*

Signed

Date