Staff Acceptable Use of ICT Policy

Date Adopted: 19th January 2022
Author/owner: Board of Trustees
Review: January 2024

NB. 'Trustees' means the Directors referred to in the Trust's Articles of Association

History of most recent policy changes

Version	Date	Page	Change	Origin of Change e.g. TU request, Change in legislation
V1.0	January 2022		New policy introduced for the Tarka Learning Partnership Central Trust Team and Schools within the Trust	Requirement for central policy to set guidance and expectations for the acceptable use of ICT by staff in the Trust and Schools within the Trust.

Contents

1.0 Introduction

The Tarka Learning Partnership and its schools seeks to embrace the use of ICT to enhance teaching and learning and the administrative processes.

This policy covers staff currently employed by the Trust, volunteers, workers and DPSCITT trainees. The policy also includes those colleagues who are contracted to work within the Trust but have not yet taken up a post (this allows pre-employment work to be undertaken using our ICT facilities). In this policy the term "staff" refers to all the personnel in this category.

The aim of this policy is to ensure that:

- Data access and use conform to regulations in regard to the Data Protection Act and General Data Protection Regulation (GDPR).
- Information relating to the use of ICT, information security and Data Protection is readily available to the relevant users throughout the Tarka Learning Partnership and schools.
- Confidentiality is always maintained.
- The integrity of the information is maintained.
- Undesirable and potentially harmful consequences associated with breaches of information security are avoided. This includes but is not limited to; bad publicity, fraud and illegal use of personal data.
- Staff, workers, trainees and volunteers understand their responsibilities online to ensure the welfare and safeguarding of pupils.
- Staff, workers, trainees and volunteers understand the boundaries of acceptable behaviour, to mitigate the risk of inappropriate communication taking place between staff and pupils and allegations being made against staff.
- Staff, workers, trainees and volunteers understand their responsibilities to keep the Trust's IT systems safe from cyber threats to prevent loss of data, disruption to business continuity and minimise financial losses

This policy applies when using Trust and school computers, using personal devices connected to the Trust or school's wireless network and when representing the Tarka Learning Partnership. The Trust's Information Security Policy is available to all staff which gives further guidance on operating within the law.

All staff and people offering services for the Trust and its schools, who access the Tarka Learning Partnership's IT systems are required to read and comply with this policy. Failure to comply with the policy may lead to an investigation and hearing under the Tarka Learning Partnership's disciplinary procedure or other appropriate action.

2.0 Responsible Use of ICT

Staff are expected to use the Tarka Learning Partnership's and the schools' IT systems responsibly and primarily for the purposes of their job.

Staff should be aware that access to the network and use of systems such as email and internet access is monitored and may be shared with their line manager or senior management.

Staff should not attempt to browse internet sites or access content that is illegal, offensive or indecent. This includes content that is pornographic or that promotes violence, religious extremism or discrimination. If staff do so, the Tarka Learning Partnership staff Disciplinary Policy will be followed.

Staff should not upload or post aggressive or offensive material online (for example material that is racist, sexist, homophobic or in any way discriminatory or liable to incite violence or hate crimes). The Tarka Learning Partnership has a Social Media policy which guides and advises staff on the acceptable use of Social Media.

3.0 Data Protection

Staff should understand their responsibilities when accessing, using and sharing Trust and school data and only do so according to Tarka Learning Partnership and school policies, including TLP's Data Protection Policy, and the Data Protection Act 1998 and GDPR guidelines.

Unless otherwise stated school data (for example personal information relating to staff or pupils, work submitted by students, internal examinations, financial data or confidential minutes) must only be stored and processed on school computers and systems (e.g. Bromcom, Office 365, G Suite, work emails and network drives).

Staff should be mindful of using systems containing sensitive information in the presence of students, parents or visitors, particularly if the computer is connected to a projector.

If a member of staff is aware that school data, particularly staff or pupils' Personally Identifiable Data (PID), has been or could be accessed by an unauthorised source (e.g. due to loss of equipment containing data), they should inform the school's Data Protection Lead immediately who will contact the Trust's Data Protection Officer and Data Protection Lead.

When leaving a computer staff should always make sure that they have logged off or that the computer is locked.

4.0 IT Security

The security of the Tarka Learning Partnership and schools' IT systems is the responsibility of all staff and staff should follow the advice and guidance specified within their work setting by the Head Teacher or IT department.

Staff must only log onto Trust and school IT systems using their own username and password.

Staff must never share their username and password with anyone else and should be aware that the Trust or school will never ask them for their password.

Staff must not make changes to the configuration of school IT equipment, including downloading or installing software, without first consulting the Head Teacher or staff responsible for IT.

Staff must not attempt to circumvent the Trust/school's IT security controls or seek to gain unauthorised access to data.

Staff should not attempt to bypass the school's internet filtering system.

All IT equipment and software purchases must be placed by the member of staff responsible for finance to ensure compatibility and security. For record keeping purposes, on arrival school owned devices must be processed by the person responsible for recording assets onto Parago.

Work IT devices allocated to staff for use off-site must be signed for by the member of staff and the device serial number recorded

If the device is lost or stolen this must be reported to the police and Head Teacher at the earliest opportunity. A crime reference number should be obtained

All files and documents should be stored on the school's secure cloud document library. No personal information should be stored on the device desktop or local drive. The download file should be deleted daily.

5.0 Cyber Security

The Trust's IT system uses Microsoft Exchange Online Protection mail filtering service. [For academies still using the Google platform, spam filtering is also a built-in feature.] This service reduces the amount of malicious, spam and spoofing emails but users should still be aware of how to recognise malicious, spam, spoofing or phishing emails and delete them or report them immediately without opening them. These emails will contain attachments, embedded links or a request for information that can cause significant harm to the IT systems or make the Trust vulnerable to fraud.

Spam takes the form of unsolicited emails from companies offering 'discount prices' or 'free software', delete them.

Spoofing and phishing emails take the form of pretending to be a bona fide company or person. Beware of emails claiming to be a bank or a company attaching an invoice, request for overdue payment or a request for information. These emails may contain spelling mistakes, look unprofessional, have an unusual email address or just not feel right. Do not open, report them by forwarding to report@phishing.gov.uk

Email addresses are sometimes hijacked to send malicious emails that may contain harmful material. If you receive an email from a colleague or other trusted organisation that appears unusual or suspicious, alert and check with the sender before opening it. If their email has been hijacked they are then able to take action to secure their email account.

If you are in doubt as to the authenticity of an email or embedded link, do not open or click on it. If you do not feel confident to delete it then refer to the Senior Leadership Team.

The Trust recognises that malicious emails can appear bona fide and that sometimes these emails may be opened in error. Where this happens, it is important that it is immediately reported to a member of the Senior Leadership Team and IT Support. This will enable the school to minimise any risk to its IT systems and protect its data.

The Trust's Cyber Security Policy is available to all staff which gives further guidance.

6.0 Use of email

The content of an email may constitute another person's personal data and therefore be subject to the provisions of the data protection act. Similarly, any email may need to be disclosed in the case of legal

action. Staff should, therefore, assume that the content of any email may be seen by others including the subject of the email.

Staff should remain mindful that email is not a secure form of communication. Other forms of communication should be considered for sending confidential or sensitive information. If in doubt, staff should seek advice from the school's data protection lead.

Consideration should be given by staff to the number of emails that they send, ensuring that all methods of communication are used appropriately and alternative methods of communication are considered. The Trust and school places no expectation on colleagues to respond to emails outside of their normal working hours. This applies also to weekend and holiday periods.

Staff must communicate in a polite and respectful way when sending an email and observe appropriate etiquette in the use of email (Appendix 1).

7.0 Safeguarding and conduct with pupils

Staff should understand their responsibilities with regard to safeguarding and understand that these also apply when using ICT.

If a staff member suspects that illegal content has been accessed using a Trust or school computer, or that a school system such as email has been used inappropriately, staff should contact the Data Protection Officer or Head Teacher immediately. Staff must not attempt to access the content as this could corrupt any evidence.

Pupil data, including Personally Identifiable Data (PID), photographs and audio/video recordings ideally will be stored on school systems and not posted/uploaded to the internet except where the appropriate consents have been obtained. Staff using their own devices to support school work should delete any data at the earliest opportunity.

In accordance with the Staff Code of Conduct, Safeguarding and Child Protection Policy and Social Media Policy staff should never give out their personal mobile, email or home telephone numbers to a pupil. School phones should be used on trips to avoid staff having to give out their personal phone number to pupils and parents. If staff are required to communicate with pupils using their own device, communication should be via the school email or MIS system.

Photographs or audio/video recordings of students should only be taken using school equipment. Staff must not use their own cameras or phones or store photographs or audio/video recordings on their own computer or memory cards.

Staff should always avoid any online (as well as offline) conduct that could be interpreted as a sexual advance or "grooming" and avoid words or expressions or any behaviour online (as well as offline) that could be interpreted as having any sexual innuendo.

Guidelines on the use of social media are outlined in the Tarka Learning Partnership's Social Media Policy.

8.0 Use of Trust or school's ICT facilities for personal use

It is understood that staff may occasionally need to use the Trust or school's ICT facilities for personal, non-school related use. Such use should be kept to a minimum so as not to interfere with work and

responsibilities and limited to break times or outside of staff working hours. Staff should also remain mindful that information or messages sent through school facilities may be attributed to the school. If Trust or school IT is used for personal use, any personal views should be stated as such.

Staff may use printers and photocopiers for personal items on an occasional basis. However, these facilities are provided to users primarily for school-related work.

Staff should not save personal files on the school network such as personal photos, music files etc. Disciplinary action may be taken if it is established that school ICT facilities have been used to excess for personal use.

Any ICT equipment which is the property of the school must only be used by the employee, trainee or worker to whom the equipment has been assigned. It is strictly prohibited for anybody to use a device which belongs to the school or Trust who has not been given permission to do so, such as a partner or family member of an employee.

9.0 Use of personal devices in school

Staff may use their own personal devices (laptops, tablets or smartphones) in school on the understanding that the security of the device is their own responsibility and that the Trust or school accepts no liability if the device is lost, damaged or stolen. Staff devices that are used to access school resources or data should be protected by a minimum 6 digit/character passcode.

Personal devices may be connected to the Trust or school's wireless network in order to access the internet and school systems.

Personal devices should be password protected and have up to date antivirus software and security updates.

School IT support will help staff connect their device to the school's wireless network and access school systems and email but cannot provide support for the device.

USB drives are not to be used. If a colleague has no other option than to use a USB or mass storage device then express permission must be obtained from the IT Support & Head Teacher and the reason recorded. The drive used must be encrypted. Data must be deleted from the drive as soon as it is no longer required and date of deletion recorded.

Visitors should be encouraged to email any electronic materials to a named contact within school prior to their visit or access them from their personal device whilst on site. If a visitor is using a USB drive, this must be scanned prior to opening any files on the drive.

10.0 Use of social media

The Tarka Learning Partnership's Social Media policy is available for all staff. The policy outlines guidance on the use of social media and networking sites.

11.0 Monitoring

The Trust's internet filtering system detects attempts to access websites or materials considered to present a risk of harm and will automatically generate an alert to the school's safeguarding team. If it is

discovered that any of the systems are being abused and / or that the terms of this policy are being infringed, action may be taken which could result in dismissal, termination of an engagement or other legal action. The Trust may also share our filtering reports with external services to help identify inappropriate or safeguarding issues.

Appendix 1 – Email protocol guidelines

Sending emails

- Email should be used to ask specific questions or to convey specific information.
- Wherever possible, use face to face communication rather than email.
- Before sending an email, consider the use of other ICT systems (e.g. staff briefing, Microsoft Teams sharing a document via MS365 or the Google drive).
- Staff should never write or send an email when they feel angry or emotional.
- Avoid open questions on email, e.g. 'does anybody know what the policy is on…'
- Avoid using all upper case or bold type as this can be interpreted as shouting.
- Consider the time that an email is being sent and consider sending it during normal working hours by putting a delay timer on it being sent.
- Avoid sending an email to a number of people because there is uncertainty over who should be dealing with the issue. It is more efficient to ascertain who the appropriate contact is before sending the email.
- Avoid prolonged discussions on email that could be better dealt with face to face or on the phone.
- Think carefully before copying emails to others. Line managers are responsible for passing on information to their direct reports as appropriate and therefore the sender does not need to do this for them.
- Think carefully before sending emails to parents and carers. Separate emails should be sent to each parent/carer to avoid divulging details of email addresses when this is not wanted, it may compromise their wishes and their safety.
- Use the BCC function to hide email addresses when sending emails to multiple users whose data should be protected OR consider using Bromcom to send group emails to parents to ensure privacy and data protection. Office staff can advise and support staff with this.

Managing your inbox

- Conduct a regular housekeeping exercise to completely clear your inbox.
- Set up an appropriate filing system to store and retrieve old emails.
- Check email regularly but not obsessively.
- Once an email has been dealt with, delete it from the inbox or file it if it needs to be retained.

The Trust's Records Management Policy is available to all staff which gives further guidance on use of emails.

Appendix 2 – Employee guide on using social media

This guidance is intended to provide best practice considerations and potential implications on employment.

- Employees should exercise reasonable professional caution in their use of all social media, including written content, videos or photographs, and views expressed.
- Employees should consider the security settings of their account and personal profiles.
- Employees must only contact students via Trust authorised mechanisms. At no time, in any circumstances, should personal accounts on social media platforms be used to communicate with pupils (including ex/former pupils).
  However, if the friendship, contact and communication on social media is due to a recreational/sports activity, community or family circumstances not a result of a former pupil/staff member relationship, the employee can use their discretion in accepting these social media contacts.
- Employees must report to the Head Teacher/Designated Safeguarding Lead any contact by a pupil by an inappropriate route.
- Employees should consider including a disclaimer on their personal social media profile to clearly identify that the account does not represent the Trust's views or opinions. For example: *'The views expressed are my own and do not reflect the views of my employer.'*

The intention of this guidance is to provide clarity on the considerations for reasonable professional caution in posting on social media however it is recognised much of this is down to perception and common-sense approaches. In particular, any ***content that is inappropriate*** should not be included in messages, status updates or links to other materials.

Inappropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs. This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs in support of proscribed terrorist groups or organisations, national origin, disability, sexual orientation, or any other characteristic protected by law.

Use During the Working Day

Systems across the Trust and its devices may provide access to the internet and social media platforms for employees to reasonably use during their break times. In addition, individuals may have access to their own devices while at work, such as mobile phones or tablets.

However, it is expected that employees act responsibly and ensure their productivity isn't affected by such use. Using social media during normal working time is inappropriate use may be considered a disciplinary matter.

Monitoring

The Tarka Learning Partnership's ICT and internet resources (including computers, smart phones and internet connections) are provided for legitimate business use and any personal use should be limited to the employee's non-working time. The Trust therefore reserves the right to monitor how social networks are used and accessed through these resources.

Any such examinations or monitoring will only be carried out by authorised staff and reported to the senior manager of the individual employee for consideration on appropriate action which may include performance management or disciplinary matters in accordance with the relevant policies.

It should be noted that the Trust can be legally compelled to show that information to law enforcement agencies or other parties as applicable.

Appendix 3 – Staff Acceptable Use of ICT Policy Agreement

I understand that I must use Tarka Learning Partnership and school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that the young people receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

Safety for my professional and personal:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, tablets, etc.) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I understand my role in keeping the school's IT systems protected from cyber threats
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident; I become aware of, to a member of the Senior Leadership team.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images.
- I will always ensure that colleagues are aware if I am recording a meeting or telephone call
- I will only use chat and social networking sites in school in accordance with the Tarka Learning Partnership policies.
- I will not engage in any on-line activity that may compromise my professional responsibilities or bring the Trust or school into disrepute.
- I will only communicate with young people and parents / carers using official school systems. Any such communication will be professional in tone and manner.

- If the data on any device is breached I will report it to the Senior Leadership Team

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal handheld / external devices (iPads/laptops/mobile phones) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not open any attachments to emails or click on any embedded links within emails or websites, unless the source is known and trusted, due to the risk of the attachment/link containing viruses or other harmful programmes.

- I understand the importance of saving work to the schools shared document library

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in Trust/school policies.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself, or others, as outlined in the Tarka Learning Partnership's Data Protection Policy. Where personal data is transferred outside the secure school network, it must be encrypted.

- I understand that the data protection policy requires that any staff or young person's data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law, or by school policy, to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.

- It is my responsibility to understand and comply with current copyright legislation, including copying of music files and video.

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use of ICT Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school, and my use of personal equipment in school or in situations related to my employment by the school.

- I understand that any electronic communication or document is open for public access/accountability and scrutiny via such legislation as the Freedom of Information Act and Subject Access Requests

- I understand that if I fail to comply with this Acceptable Use of ICT Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Trustees/Governors and in the event of illegal activities the involvement of the police.

Acceptable Use / Bring Your Own Device Considerations - Staff

The Tarka Learning Partnership recognises that many staff choose to access school information from their own devices.

Any member of staff wishing to do this must be aware that they have a direct personal responsibility for ensuring that the device they choose to use has the benefit of encryption that is above and beyond a simple password protection.

Staff must ensure that personal devices such as mobile smart phones, tablets and other portable electronic equipment are set to lock and only open with encrypted passcodes to prevent unauthorized access.

Staff must not use removable or portable drives.

School will support and enable staff to ensure that their devices are compliant.

Staff are advised not to take any data off site to minimize the risk. If data must be taken off site it must be secure at all times and is the responsibility of the member of staff.

If any member of staff uses a device without these safeguards in place it will be a disciplinary breach if data is unlawfully accessed by a third party.

Non-Compliance Protocol

It is important that any non-compliance is brought to the attention of the Data Protection Officer and Head Teacher to enable an action plan to be developed and implemented. This record will also serve as a useful mechanism to identify trends, risks and potential breach hazards.

By having an agreed timescale for review, identifying training needs that may be applicable to an individual or group of people will assist future compliance.

……..

I have read and understand the above and agree to use the Trust/school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff Name ……

Signed ……

Date …….