




The Park Federation Academy Trust
Internet and E-mail Policy
2020

Version	Date	Status and Purpose	Changes overview
1	15 September 2016	Draft for comment	
2	08 October 2016	Approved	
3	29 October 2018	Periodic review	
4	September 2019	Periodic review	
5	July 2020	Periodic Review	KCSIE 2019

Approval

Signed by the CEO and Federation Principal on behalf of the Board of Directors	 Dr. Martin Young
Date of approval	July 2020
Date of review	July 2021

Notes on Document Control

This document is the property of TPFAT (The Park Federation Academy Trust) and its contents are confidential. It must not be reproduced, loaned or passed to a 3rd party without the permission of the authoriser.

It is controlled within the Park Federation Academy Trust Admin Server where the electronic master is held and can be accessed on a read only basis, subject to security permissions.

Users of the document are responsible for ensuring that they are working with the current version.

Paper or electronic copies may be taken for remote working etc. However, all paper copies or electronic copies not held within the Admin Server are uncontrolled.
Hence the footer 'DOCUMENT UNCONTROLLED WHEN PRINTED' which must not be changed.

Once issued, as a minimum this document shall be reviewed on an annual basis by the originating team/function. Any amendments shall be identified by a vertical line adjacent to the right hand margin.

To enable continuous improvement, all readers are encouraged to notify the author of errors, omissions and any other form of feedback.

Contents

	Page
Operational Summary Policy Aim	4
Policy Summary	4
Access Summary	4
Wireless Summary	4
Introduction	5
Purpose	5
Scope	5
Explanation of Terms	6
Responsibilities	6
Misuse	6
Access to E-mail Messages	7
Internet Access Principles	7
E-mail Access Principles	8
E-mail Encryption	9
E-mail Security	9
E-mail Protection	9
E-mail phishing guidance	11

Formatted Table

Legal Framework:

Data Protection Act 2018

The General Data Protection Regulation

Computer Misuse Act 1990

Human Rights Act 1998

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Education Act 2011

Freedom of Information Act 2000

The Education and Inspections Act 2006

Keeping Children Safe in Education 2019

Searching, screening and confiscation: advice for schools

Associated Documentation and Policies: The Park Federation Academy Trust (TPFAT) Policies. Disciplinary Policy, Data Protection Policy, E-Safety Policy, Remote Access Policy, Staff Code of Conduct, Social Media Policy. Information shared is subject to copyright, data protection, freedom of information, equality, safeguarding and other legislation.

Operational Summary Policy Aim

To set standards for the use of the Internet and E-mail services provided by The Park Federation Academy Trust.

Policy Summary

This policy is designed to help staff understand TPFAT's expectations for the use of the Internet and E-mail and its response to inappropriate use.

What it means for staff - All staff employed by TPFAT, whether permanent, temporary or external contractors are expected to adhere to the policy and the protocols and procedures.

All TPFAT Employees - are responsible for reading this policy to maintain current awareness of changes which impact on their roles.

Access Summary

Our service VPN network is hosted through TrustNet and internet filtering is provided through TrustNet (LGFLv2) and Atomwide.

All PCs on our network are protected using Sophos anti-virus, all access to the internet is filtered using multiple streams including key-words, word-group blockings and internet site blockings.

Any network devices that accesses services or internet using hardwired or wireless services within our academies are subjected to the same filtering policy as any other devices on our network. This would cover BYOD (Bring Your Own Device), e.g. laptops, tablets and mobile phones.

Many sites from the internet are filtered and therefore automatically blocked and cannot be unblocked.

Academies and schools work at "Secure and Detection level 3". This means that every effort is made to secure our systems internally and the same effort is given to detection of intrusion of our systems externally.

A copy of the **Category Definitions** from LGfL can be made available and put into a word document and stored on our network. The categories allow us to state that we are compliant with the "UK Safer Internet Centre" safeguarding of children and staff using our internet service.

Wireless Summary

1, TPFAT-Staff. Users (with an account on our domain) using TPFAT-Staff will be able to gain access to our network services through network authentication.

2. TPFAT-Student. Users (with an account on our domain) using TPFAT-Student are restricted to the pupils' area which is only accessed by network authentication.

3. TPFAT-Guest. This account will give a user restricted internet access only, at the same time bypassing our network domain, (not visible to the user).

Introduction

Access to the Internet and communication by E-mail has increasingly become an essential part of modern day business within TPFAT. The advantages that these electronic modes of communication offer are obvious; however, less apparent is the threat of misuse that such media poses.

The use of all installed systems/connections is for legitimate work related purposes only and is encouraged to improve the quality of work and productivity in education and training. Therefore, we have a responsibility to ensure that the use of information technology is not misused and maintains confidentiality, whilst at the same time producing secure and accurate work.

Staff should be aware that all E-mail messages are subject to, but not limited to, the Data Protection Act (2018) and the Freedom of Information Act (2000). E-mails can form part of a personnel record or corporate record, and as such it is important that E-mail messages are used and managed efficiently. E-mail messages are considered to be a legally binding form of communication and as a result may be used as evidence in any legal action taken against TPFAT or individual employees.

This policy is designed to help you understand TPFAT's expectations for the use of the Internet and E-mail and its response to inappropriate use.

All staff employed by TPFAT, whether permanent, temporary or external contractors are expected to adhere to the policy and the protocols and procedures that are in place to support this policy document.

Purpose

The purpose of TPFAT Internet and E-mail Policy is to:

- Set standards for the use of the Internet and E-mail services;
- State the position of TPFAT on communication via E-mail and the Internet;
- Set out the obligations that staff have when using the Internet and E-mail facilities;
- Ensure that Internet and E-mail facilities are used in a way that will not breach legislation or TPFAT policies.
- Ensuring that all employees are aware of their obligations as users of the Internet and E-mail facilities;
- Ensuring that all employees understand what is meant by acceptable use of TPFAT's Internet and E-mail facilities;
- Ensuring that appropriate and effective monitoring systems are in place;
- Ensuring staff confidentiality is maintained,
- Ensuring that appropriate action is taken by TPFAT management where misuse of the Internet and or E-mail facilities are encountered.

Scope

This policy applies to all Internet, Intranet and E-mail systems and services managed and/or owned by TPFAT.

All users of TPFAT's Internet, Intranet and E-mail systems and services are expected to comply with this policy.

Explanation of Terms

Offensive material - can be described as any material that includes for example, hostile communication (audio, video, text and images) relating to gender, race, sex, sexual orientation, religious or political convictions and disability.

Harassment - is when someone behaves in a way which makes you feel distressed, humiliated or threatened. It could be someone you know, like a member of staff, service users or it could be a stranger.

Responsibilities

Organisational Responsibilities

- Establish adverse incident and investigation procedures for the reporting of all breaches of this policy through the appropriate management channels;
- Ensure that line managers understand their responsibilities for the implementation of this policy within their business or clinical area and that their managed staff adhere to the principles;
- Ensure that controls are in place for the physical environment to prevent unauthorised access to the computer systems that allow access to the E-mail and Internet system;
- Compliance with section 46 of the Freedom of Information Act, Code of Practice on Records Management with relation to disclosure of E-mails.

Line Managers Responsibilities:

- Informing the IT Network Manager of staff who are expected to be absent for a significant period of time, so that their E-mail accounts can be disabled until the member of staff returns to work (e.g. maternity leave, long term sickness);
- Informing the Network Manager and HR Department of staff members who have left TPFAT.

ICT Responsibilities

- The IT Network Manager is responsible for the overall integrity and security of the network including its computer systems and ensuring that TPFAT's E-mail environment is maintained effectively and securely;
- Ensuring Internet website access is controlled preventing inappropriate and potentially infected websites being viewed on TPFAT computers. The responsibility for accessing inappropriate sites ultimately lies with the user;
- Manage the systems and services used in providing the E-mail and Internet services within TPFAT's ICT domain.

Users Responsibilities

- The school provides each member of staff with an individual email address.
- This email account should be used for work purposes only.
- All work-related business should be conducted using the email address the school has provided.
- Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.
- Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
- Comply with this Policy at all times including any use of the remote service whilst off duty;
- Report any incidents such as inappropriate use or security breaches or virus infection to their line manager and IT Network Manager;
- Always ask for advice and guidance on the content of this Policy from line managers or the IT

- Network manager if unsure of the content;
- Each user is responsible for ensuring that they fully understand and comply with this Policy.
- Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.
- If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

Misuse

This policy covers all users of our school's ICT facilities, including governors, staff, volunteers, contractors and visitors. Staff members must be aware that the Internet is inherently insecure and confidential information in relation to the business of TPFAT and/or service user/another employee's identifiable information must never be disclosed or placed on Internet sites or web applications.

Misuse of E-mail and the Internet may result in legal liability for TPFAT and, in some cases, the individual user. Inappropriate use may give rise to

- Liability for defamation
- Copyright infringement
- Breach of confidence
- Inadvertently entering into contracts
- Claims of bullying, harassment and discrimination
- Claims for compensation

Breaches of this policy may be dealt with under our associated policies on Page 4.

Access to E-mail Messages

TPFAT will not normally access any individual's mailbox without the permission of that individual. However, there may be occasions when the information must be accessed by the IT Network Manager and is deemed it necessary to access a user's E-mail mailbox without the employee's permission, by Senior Managers of TPFAT e.g. Chief Executive Officer, Chief Operating Officer.

Examples of reasons for accessing an individual's mailbox are, but not limited to:

- To action subject access requests under the Data Protection Act
- To obtain Freedom of Information requests
- To obtain evidence in support of disciplinary action
- To obtain evidence in a criminal investigation
- To obtain evidence in legal proceedings
- To obtain access to TPFAT business data

Internet Access Principles

TPFAT reserves the right to restrict access to materials on the Internet where it is deemed appropriate to restrict access. This will include access to any sites considered offensive and inappropriate.

Any restrictions to materials by TPFAT shall not be deemed to impose any duty on TPFAT to regulate the content of material on the Internet. Furthermore, any lack of restriction does not mean that access to that material is authorised.

Information obtained through the Internet may not be accurate and the user must check the accuracy, adequacy or completeness of any such information. Furthermore, it is the responsibility of the user when using information obtained from the Internet to be aware of copyrighted material in accordance with the permission granted by the publisher.

The threat from viruses and security breaches from the use of the Internet are very real. Users must be aware that information downloaded from the Internet may contain hidden code capable of destroying data or interfering with the network functions. Therefore users must take great care and be vigilant when downloading any files from the Internet.

No member of staff is permitted to access, display or download offensive material. To do so is considered a serious breach of TPFAT Internet and E-mail policy and following an appropriate investigation may result in disciplinary action being taken against the individual.

Users of TPFAT Internet connection must not:

- Circumvent or attempt to circumvent any of the security controls put in place by TPFATs IT Network Manager;
- Download any executable or scripting programme on to TPFAT computers;
- Supply any personal details, including but not restricted to, name, address, credit card details etc. whilst accessing websites;
- Download copyright material such as music, pictures, text, software etc. This is a breach of copyright law;
- Breach the Computer Misuse Act (1990) or the Data Protection Act (2018), for example, passing pupil related data to inappropriate parties.

Usage of YouTube for Education

YouTube—Videos on the file-sharing website YouTube can be used to effectively support many areas of the curriculum. The popular site contains a selection of videos which cover the range of topics focused on across the schools within The Park Federation Academy Trust – most noticeably, Science and History topics. Additionally, there is a variety of music, song and dance performances appropriate for children. When these videos are used safely and appropriately, they can be an extremely beneficial resource for Class Teachers and Support Staff.

Formatted: Left, Indent: First line: 0 cm

However, there are potential risks when working with YouTube that staff should be aware of. For example, despite a filter/flagging policy being in use on YouTube, inappropriate images, unsuitable written comments, or bad language can still all be accidentally revealed to the children. In order to prevent this from happening, the following precautions should be taken:

Finding suitable videos:

- Searches, or first observations of a potential video, should not be carried out with any child in the class room.
- Before showing a video to the class, the video should be watched and listened to carefully by the Class Teacher or TA, who should look out for inappropriate content material along with any inappropriate comments that appear underneath the video.
- It is the class teacher’s responsibility to make the final approval of a video.

Playing the video for the children:

- Using the remote control, the Smartboard should be frozen, stilled or muted (depending on the option available on your remote) prior to Full Screen mode being selected for the video. (This is so that no comments or any other videos can be seen by the children).When the video is ready, the Smartboard can be unfrozen and the video watched.

- Before the end of the video, pause it so 'recommended' videos that might potentially contain inappropriate language, are not revealed.
- When the video is finished, the Smartboard should once again be frozen, stilled or muted (or even turned off) so that the video can be exited and the YouTube window closed safely.

Should any inappropriate content be shown this MUST be reported to your Head teacher/Principal immediately and an email also needs to be sent to Alex James (Federation the IT- Network Manager) so that the content can be blocked through the Federation filtering system.

E-mail Access Principles

TPFAT's E-mail system should be utilised as a formal communication system.

TPFAT provides each user a unique E-mail addresses which always end with the suffix "*@theparkfederation.org*".

E-mail Encryption

Google mail is an encrypted and secure online mail system.

E-mail Security

Users must not share their username and password with any other person and should not leave their computers unattended whilst logged on, as they will be held responsible for any activity which takes place using their account.

If you are leaving your computer for even a short period of time, you should ensure that your E-mail account is not left open and accessible. You can do this by locking your workstation - (***press Ctrl-Alt-Delete and choose Lock this Computer***).

If you see someone else's e-mail software left open on a computer, you must not read or view their E-mails in their absence. Nor should you make any attempt to open someone else's E-mail account without their prior permission. Unauthorised use of someone else's digital identity is strictly forbidden and will result in disciplinary action.

You should not give out a colleague's E-mail address to anyone outside the TPFAT unless you are certain that your colleague will be happy for you to do so.

~~YouTube – Videos on the file sharing website YouTube can be used to effectively support many areas of the curriculum. The popular site contains a selection of videos which cover the range of topics focused on at The Park Federation – most noticeably, Science and History topics. Additionally, there is a variety of music, song and dance performances appropriate for children. When these videos are used safely and appropriately, they can be an extremely beneficial resource for Class Teachers and Support Staff.~~

E-mail is a way that computer viruses can be received, or where a system is infected, computer viruses can be spread to other systems. For this reason, it is essential for your security and the security of other TPFAT messaging service users that all files brought onto your system from E-mail, disk or other sources are scanned by an up to date, reputable anti-virus and malware package. TPFAT uses Sophos Anti-virus software on all its installed PCs. This software also includes an anti-malware tool.

To eliminate possible virus infections to TPFAT Local Area Network, all E-mail messages, which

contain any attachments, will be scanned. All incoming E-mail messages, which contain attachments, will be scanned. Any incoming or outgoing messages or attachments, which are identified as potentially harmful, will be blocked, quarantined and deleted and or examined.

E-mail Phishing Guidance

Criminals send malicious email communications all the time to extract information from individuals. This is called phishing, which means tricking you into sending them sensitive information by clicking on links or opening attachments. They also try to persuade you to inadvertently install malware on your computer. The messages they send can place your data and computer at risk to all manner of threats.

We all get phishing emails so this may help you to spot them and avoid being phished!

1: Proceed with caution!

- Emails can come from anywhere so never assume they are genuine, especially if they are unexpected.
- Pause for a moment and consider the message carefully, whatever the format.
- **DON'T** automatically click on links or open attachments.
- **DON'T** automatically reply or try to unsubscribe.
- **DON'T** automatically contact any phone numbers in the message. Look up phone numbers from an official source such as the legitimate website of the sender.
- Remember that company logos, branding and web addresses can easily be forged in messages to make them look more realistic.

2: Things you should all look out for in a phishing Email:

- Is your name missing or incorrectly spelt? Reputable companies usually personalise their communications with your name.
- Is the grammar right and are there lots of spelling mistakes?
- If it appears to be from someone you know, does it look and sound right?
- Is the message requesting personal data or bank details?
- Are you asked to do something like validate account credentials or re-activate an account?
- Are you asked to make payments immediately?
- Has the message been sent to multiple recipients?

- Did the message come out of the blue? Companies don't just contact you asking questions or offering things without you doing something first.

3: Check for hooks

- Does the sender's address match the organisation that supposedly sent the message?
- Hover over all links to check where they really go.

4: What to do when you identify a phishing Email:

- You can report all suspected spam, phishing by forwarding it to ajames@theparkfederation.org then delete it from your "Inbox, Sent and Deleted item".
- All cyber spam, phishing is reported to https://www.actionfraud.police.uk/report_fraud