STAMFORD PARK TRUST

Stamford Park Trust

IT Acceptable Use Policy

May 2023

Policy Title:	IT Acceptable Use Policy
Document Reference:	SPT/POL/000107
This policy applies to:	All staff and students
Owner/Author:	Chief Operating Officer/Head of IT
Establishment Level:	Trust
Approving Body:	Executive Team
Review Cycle:	Annual
Date approved:	26th May 2023
Date of Last Review (this should be the date on the cover):	May 2023
Summary of Changes:	New policy bringing together previous separate staff and student policies
Date of Next Review:	May 2024
Related Documents/ Policies:	JANET Guidelines & Acceptable Use Policy Trust Safeguarding Policy Trust Code of Conduct Policy
Legal Framework/Statutory Guidance:	The Computer Misuse Act, 1994 The Data Protection Act, 2018 EU General Data Protection Regulations (GDPR), 2018 Regulation of Investigatory Power Act, 2000 The Telecommunications Act, 1996 The Copyright, Design and Patents Act, 1998 Keeping Children Safe in Education

Contents

1 Introduction

1.1 The Trust's Acceptable Use Policy (AUP) has been drawn up to protect all parties – the students, the staff and the Trust. The computer systems are owned by the Trust and are made available to staff and students to enhance their professional and pedagogical activities, any person using IT facilities must abide by the Trust's Acceptable Use Policy.

2 Security

2.1 User Accounts

Only the named account user should use their account on the computer network.

The owner of the account must take all reasonable steps to protect and maintain the security of any passwords allocated for their use. Specifically, they should not:

- Disclose their passwords to anyone else.
- Allow anyone else to access a computer using their account.
- Log on to the network using another person's account.
- Leave a computer unattended without first logging off or locking the device.

Account users who suspect the integrity of their password has been compromised should change it immediately and inform the IT team.

2.2 Data Storage

All users are allocated a user 'home directory' in which to store their personal files. Departmental 'Shared Work' areas are also provided to enable colleagues to share resources as appropriate. Users should not attempt to access directories and files for which they are not authorised. In particular, the confidentiality of data belonging to other users must be respected.

Data storage is a finite resource. Disc quotas are in place to control and manage the storage space available and users will not be allowed to exceed this limit. It is the user's responsibility to ensure good house-keeping of their home directory by deleting unnecessary files and regularly emptying their Recycle Bin.

Because storage space is limited, users should exercise restraint in saving files. The downloading of music, games and executable (program) files is not allowed. Any music or games found in user's folders will be removed by IT staff.

All users have a Microsoft Office365 account; while this has been implemented primarily for its messaging services (e-mail, calendaring, etc.) it also provides each user with 'OneDrive for Business' storage. All users are encouraged to make full use of its capabilities; for example, storage of raw source image files for photography, etc.

2.3 Software

All software will be installed by IT staff. If any user requires software to be installed it should be forwarded to the IT helpdesk email address with the appropriate licence.

Users must not use the Trust's equipment to run any software other than that provided by the Trust on the particular machine. This includes music, videos, games or other software available via the Internet or other third parties.

Users must not attempt to install or uninstall any executable files on to, or from, a trust computer.

Users must comply with their legal obligations concerning copyright. Under no circumstances may any of the equipment in the trust be used to make copies of software or other data without the authorisation of the copyright holder.

2.4 Viruses

Users must take all reasonable steps to exclude and avoid the spread of malicious software and must co-operate with measures instituted by the Trust to prevent the spread of such software.

All Trust computer equipment is protected against malicious software by up-to-date Anti-virus protection software. All users are strongly advised to ensure that their home computers are protected with suitable anti-malware software.

2.5 Hardware

IT hardware must be treated with care and used only in accordance with its proper operating instructions. Problems with equipment should be reported to the IT helpdesk. Users must not move or remove equipment, unless designed for this purpose e.g. laptops, tablets.

Users who need to access Trust resources remotely must do so via Trust portals and approve methods of access.

3 Internet access and e-mail

3.1 General Points

Trust staff and students have access to the Internet and email. However, such widespread Internet and e-mail access opens up the Trust to risks and liabilities. It is therefore essential that all users read these guidelines and make themselves aware of the potential liabilities involved.

Staff will support the Trust safeguarding approach and will report any behaviour which may be inappropriate in line with Trust safeguarding procedures.

The Trust has the right to monitor all aspects of its telephone and computer systems that are made available to users, and to monitor, intercept and / or record any communications made by users, including telephone calls, e-mail or Internet communications. In addition, the Trust wishes to make you aware that closed circuit television (CCTV) is in operation for the protection of employees and students.

Computers and e-mail accounts are the property of the Trust and are designed to assist staff and students in the performance of their duties and studies. There is, therefore, no guarantee of privacy in any e-mail sent or received.

Sites and materials accessed must be appropriate to the educational ends for which they are provided. Inappropriate use of the Internet and e-mail is considered to be the downloading or transmitting of any material which might reasonably be considered to be pornographic, obscene, abusive, sexist, racist, or defamatory. This includes content circulated in emails, regardless of the point of origin.

Use of the Trust ICT systems and equipment for personal financial gain, gambling, political purposes or advertising is forbidden.

Use of the Trust ICT systems to breach any laws or which threaten the safety and security of students at the academy may result in professional sanctions as well as potential legal actions.

3.2 Filtering & Monitoring KCSIE guidelines

Reasonable private use of the Internet is permitted, but should be kept to a minimum and should not interfere with Trust work. Excessive private access to the Internet during working hours may lead to disciplinary action and may, in certain circumstances, be treated by the Trust as gross misconduct.

The sites accessed by users must comply with the restrictions set out in these guidelines. Accessing inappropriate sites may lead to disciplinary action and may, in certain circumstances, be treated by the trust as gross misconduct (see paragraph 3.1.4).

The use of the Internet, e-mail and wireless access during 'out-of-hours' times such as breaks and lunchtimes is not regarded as different to its usage at any other times.

The Trust has implemented a web-site blocking facility in order to restrict access to those web-sites deemed inappropriate. However, due to the international scale, the linked nature of information and the almost exponential growth of content available via the internet, it is not possible to guarantee that unsuitable material will never appear on a computer. The Trust cannot accept liability for the material accessed, or any consequences thereof.

In the event that distasteful or unacceptable materials do slip thorough the firewall then users should contact the IT helpdesk in order that the content can be blocked as a matter of urgency. Conversely, if any member of staff should come across a web resource that is blocked unnecessarily then they should also contact the IT helpdesk so that the resource may be investigated and unblocked if appropriate.

The accessing of websites of an inappropriate nature will be treated as serious breaches of this Policy. Such misuse of the computer systems will be treated by the trust as misconduct and will, in certain circumstances, be treated as gross misconduct. The trust reserves the right to use the content of any user's e-mail in any disciplinary process.

The accessing, or attempted access, of websites which are deemed to be extremist in nature or concerning online behaviours evidenced through the trust web filtering system will be referred to the trust Safeguarding teams.

In accordance with the Prevent Duty web filters are in place to track and block any attempts to access websites linked to terrorism, extremism or radicalism.

In accordance with the governments Keeping Children Safe in Education policies filtering & monitoring systems are in place within each of the academies. Trust staff who observe students breaching the guidelines should report the occurrence to the safe guarding team using the appropriate system in place.

3.3 Use of e-mail

E-mail messages should be drafted with care. Due to the informal nature of e-mail, it is easy to forget that it is a permanent form of written communication and that material can be recovered even after it has been deleted from the user's computer.

The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded.

Users should not make derogatory remarks in e-mails about staff, students, or any other person or organisation. Any written derogatory remark may constitute libel. Emails may also be released to named individuals where a subject access request is made under the General Data Protection and GDPR Regulations.

Users should utilise secure email systems to send communications that may contain sensitive or personal information.

Users should not create e-mail congestion by sending trivial messages, unnecessarily copying e-mails or forwarding 'chain mail'. Users should also regularly delete unnecessary e-mail to prevent overburdening the system.

Trust e-mail systems should be utilised for the business of the Trust and not personal use. Users should exercise judgement and avoid any communications that could lead to reputational damage.

3.4 Copyright and Downloading

Copyright applies to all text, pictures, video and sound, including those sent by e-mail or on the Internet. Files containing such copyright-protected material may be downloaded, but not forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.

Copyrighted software must never be downloaded. Such copyrighted software will include screen-savers.

3.5 Social Media

The Trust is keen to embrace social media technology and support its use both as a communication tool and as an innovative learning resource. Social networks can improve wider participation in an area such as Tameside in addition to opening up opportunities for learning to take place outside of the classroom environment.

Due to Social Media's ubiquitous use as a tool for sharing personal opinions and life events it is therefore necessary to offer guidance to teachers on managing its use with a common-sense approach. This policy is designed to ensure that any potential risks to Trusts staffs or reputation are protected from legal, ethical and/or abusive situations.

3.6 Professional Use of Social Media

Social media is one of the key communications and the marketing tools used by the Trust. Trust staff are therefore encouraged to use social media as a means of communicating and sharing with students.

Departments and individual staff members can create pages and groups to share and network with partners and colleagues from within the Trust and other institutions.

Trust staff should not allow any student to be their 'friend' or to follow their personal pages. Trust staff should never attempt to 'friend' or follow personal pages of students. The exception is for trust students who are of adult age for alumni purposes.

Best practice is for employees to create new 'work' profiles that hold little personal information for learners to follow.

Trust staff can use their own devices to access social media sites and use should be in accordance with this policy.

Staff must be aware at all times that, while contributing to the Trusts Social Media activities, they are representing the Trust. Staff who use social media as part of their job must adhere to the following safeguards:

- Making sure that the communication has a purpose and a benefit for the Trust.
- Obtain permission from a manager before embarking on a public campaign using social media.
- Report any concerns regarding other staff's or student's use of Social Media i.e. extremist activities, expression of extremist views or use of extremist language or any evidence of discrimination or failure to uphold British Values to a member of the Safeguarding Team.

3.7 Personal Use of social media

The use of social media on laptops, tablets and mobile phones is permitted within the working hours of staff, however staff must be aware that trust related use of social media must take priority.

Personal use of social media must not interfere with an individual's day to day duties within the Trust.

Excessive use of social media for personal use may, at times, be subject to monitoring, in accordance with is policy.

Where monitoring or reports indicate misuse of social media at work, a member of staff may also be subject to disciplinary procedures in accordance with the disciplinary procedure.

Students must not do anything that could be considered discriminatory against, or bullying or harassment of, any individual, whilst a member of a Social Media group, for example by:

- Making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion, belief or age.
- Using social media to bully another individual.
- Posting images that are discriminatory or offensive, or links to such content.
- Posting images of trust staff or student without consent.
- Bring the Trust into disrepute, for example by: Criticising or arguing with teachers or other students.
- Making defamatory comments about individuals or other organisations or groups.
- Posting images that are inappropriate or links to inappropriate content.

3.8 Home Working

Working at home can be helpful in promoting flexibility for staff, however this presents increased cyber security challenges that need to be managed.

Staff are able to use collaboration tools, email and other systems to communicate with each other. It is important to remember that the same work-related cyber security rules apply at home.

Devices used for working outside an office environment are more vulnerable to theft and loss. Whether using your own device or the trusts, ensure it is secure and not left unattended. If the device is portable and not being used please keep it somewhere safe.

If your work device is lost or stolen, please report it to the IT Helpdesk as soon as possible.

When working from home Staff must use Trust approved portals when accessing Trust information or data.

3.9 Online Training

All users will be asked to complete an online training course which outlines the importance of cyber security and online safety.

4 Online Teaching and Learning

The Trust will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements. Staff and students must ensure that they read and apply the guidance provided in the Trust's Safeguarding Policy and Procedures relating to the delivery of online teaching.

Staff must only use platforms specified by senior managers and approved by the Head of IT to communicate with students.

5 Monitoring

Where the Trust has reasonable cause to believe that there is a breach of this Policy it has the right to monitor and inspect any and all aspects of its computer systems. This includes, but is not limited to:

- The abuse of Internet access.
- The transmission of virus infected files.
- The sending of unwanted, inappropriate or offensive e-mails.
- Excessive use of personal e-mails.

Users should be aware that all Internet access and usage is recorded; this information includes:

- User name
- Computer name
- Web page
- Date and time

Any web site deemed to be inappropriate can and may be blocked from access within that academy. Staff should inform the IT team via the local IT helpdesk should they need access to a site that is blocked.

The Trust reserves the right to use the content of any computer logs and records or any email in any disciplinary process.

6 Legislation & Trust Policies

These guidelines comply with the following legislation:

- The Computer Misuse Act, 1994
- The Data Protection Act, 2018
- EU General Data Protection Regulations (GDPR), 2018
- Regulation of Investigatory Power Act, 2000
- The Telecommunications Act, 1996
- The Copyright, Design and Patents Act, 1998
- Keeping Children Safe in Education
- JANET Guidelines & Acceptable Use Policy
- Trust Safeguarding Policy
- Trust Code of Conduct Policy

Should there be a breach of any of the above policies by staff or students then they would be subject to the Trust disciplinary procedures.

It is the duty of each staff user of the Trust's computer facilities to ensure that their usage complies with the Data Protection Act 2018 and GDPR 2018. Password controlled access to relevant parts of the student

record systems is granted to staff by the MIS manager. Staff must ensure that such systems are used appropriately.

Computers must be logged off at the end of any session in which they are using personal data and should be locked whilst unattended during lessons to prevent unauthorised access.

Personal data should be communicated between staff via the secure student record systems rather than email.

Personal data must not be stored on any portable computer system, USB memory stick, optical disc or any other removable media.

7 IT Support Department

The IT Support department operates an IT helpdesk system. Any faults or other issues involving any aspect of the Trusts IT system should be reported via this system so that resources can be allocated and the issue tracked and monitored to ensure a satisfactory solution.

The IT Support department will provide appropriate assistance to any user. Users who require any information or help about the use or set-up of their computer should contact the local IT Helpdesk.