Tudor Park Education Trust Policy for:	Use of ICT and Internet by Staff
Person(s) responsible for updating the policy:	Chief Executive Officer
Date Approved:	Board of Directors on 7 July 2016
Date of Review:	Every 3 years
Status:	Non Statutory

Tudor Park Education Trust oversees this policy but the local governing body of each academy or school within the Trust is responsible for the implementation of the policy.

This policy should be read in conjunction with the following policies:

- Safeguarding and Child Protection.
- E-safety
- Staff email.
- Secure data handling.
- Management and retention of records.
- Use of personally owned devices by staff.

Background

Information and Communications Technology (ICT) is a vital tool in the process of teaching and learning. Teachers prepare pupils through ICT for a rapidly changing world in which many activities are transformed by access to a varied and constantly changing and developing technology.

Pupils use ICT tools to find and process information and teachers need to set an example of how this is done in a responsible manner, creatively and with discrimination. Pupils learn from teachers how to employ ICT to enable rapid access to ideas and experiences from a wide range of sources. All staff need to become confident users of ICT, so that they can develop the skills, knowledge and understanding which enables them to use appropriate ICT resources effectively as powerful tools for teaching.

ICT is also a vital tool in the administration of the school. Teachers and support staff need to be aware of what is acceptable use of the school's administrative network of computers.

Introduction

This policy is in place for use of these facilities by staff. There is a separate policy for use by pupils.

There is a network of computers which are used in the administration of the school (finances, pupil records, timetables, registers etc). Many more computers are available for use by pupils and staff and the majority of these have access to the internet through the school network. All pupils and staff have a login name, password and an email account.

The email system is available for use both from within the school and externally.

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access.
- No user should be able to access another's files without permission (or as allowed for monitoring purposes within the school's policies).
- Access to personal data is securely controlled in line with the school's personal data policy.
- Logs are maintained of access by users and of their actions while users of the system.

Objectives and targets

The objective of this policy is to develop an appropriate code of practice for use of ICT by staff at Tudor Park Education Trust.

Action plan

The following code of practice must be adhered to by staff.

All staff will be expected to sign the ICT: Staff acceptable usage agreement – see appendix 1. Staff who receive a laptop which is the property of the school will also be expected to sign the ICT: Staff laptop agreement – see appendix 2.

When signing on to the network you will be given a brief reminder of the Acceptable Usage policy and by signing in you will be bound by this policy.

Rights of access

A safe and secure username/password system is essential and will apply to all school ICT systems, including email.

All passwords are generated by the network manager/ICT technical support staff and are unique to each member of staff. Passwords can be reset by the user or the ICT Technical Team or, in the cases of students, can be reset by staff.

Users are required to change their passwords every 90 days for security purposes. Please keep your passwords secret and secure. They must not be shared with other users at any time.

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the network manager and these will be reviewed, at least annually.

Emails

Email is an essential tool at the school and all members of staff must read and abide by the separate staff email policy when managing their email accounts, sending emails, receiving emails and especially if emailing personal, sensitive, confidential or classified information.

Internet and intranet

The internet is not necessarily secure and school sensitive information could be viewed by unauthorised individuals.

Staff must abide by the current restrictions on correspondence or the passing of information to outside organisations or individuals.

Unless encrypted, the transmission of school sensitive data over the internet is strictly prohibited.

At no time may staff use the internet to send school or personal information that would, if intercepted, place the school in violation of UK laws or regulations.

Staff may not use the internet to view illegal, pornographic or seditious material that would place the school at legal risk.

Staff may not download or distribute material from the internet without virus checking. Users are advised to think carefully before opening attachments or following links from untrustworthy sources.

Staff may not use the internet in a role inconsistent with their role in the school.

Staff must not gain unauthorised access to the internet eg by hacking or by trying to circumvent any ‘blocking’ controls.

Staff must not use another individual’s user identity to access the internet or intranet.

Staff may not use the internet for private business purposes or private commercial gain.

Staff must not engage inappropriately with pupils through social networking sites. Staff must be mindful that all postings on social network sites are widely accessible. See also the social media policy.

Laptop computers

Laptops, ipads, tablets and similar devices which are the property of the school fall under the same restrictions of use as networked computers. Loss, damage or theft of a laptop through misuse, or negligence may result in financial sanctions.

Laptops and peripherals should be kept in a secure place; when not in use, it should be switched off. During term breaks laptops should not be left in offices or classrooms. If you do not intend on taking your laptop home with you it must be returned to ICT technical support for safe keeping.

Laptops and other devices that are the personal property of the individual must only be used in line with the Use of personally owned devices by staff policy.

Arrangements for leaving the College

All intelectual property (lessons plans, schemes of work, resources etc) used, created and/ or stored on the schools network remain property of the school under the Copyright Act 1976. As such staff must attempt to remove these files from the network.

Staff should make adequate arrangements when ending their contract with the school to remove all private confidential files that may be saved on either their network area or on the .\teacher log in on their laptop. Remote access to the network and email accounts will terminate on final day of employment. In extenuating circumstance you may request additional 30 days of access to the network and email. This request must be in writing and addressed to the Headteacher.

It is recommended that staff make time to transfer key documents to their line manager before leaving the college.

School owned Mobile Devices

Some staff are issued with mobile devices to support them in carrying out their role more effectively. These devices range from basic mobiles to smart phones. These phones should only be used for work purposes and are barred from making international calls. The schools current call plan allows for unlimityed minutes and unlimited texts.

Phones should be seen as an extention of the network and as such any data stored on the device and all use of the device should comply with the school acceptable usage policy.

Staff are not permitted to use ‘personal’ user logins on school owned smart phones. For example staff are not permitted to use an Apple Id associated with a privately owned device on their work phone. ICT will work with staff to support them in setting up school accounts for use on these phones.

Smart phones capable of downloading email must have passwords enabled at all times.

Phones that allow for location tracking to support ‘find my phone’ applications must have this enabled at all times.

If at any point staff lose their device the must inform ICT and work with them to remotely wipe sensitive data from the device.

Use of MIS and Financial Data

Data encryption

Transfer of data

Access restrictions

Misuse of computer systems by staff

Misuse or abuse of computer systems by staff is a serious matter and will be dealt with under the school's disciplinary procedures. The penalties for improper use may include dismissal, either with, or without notice. The following are expressly prohibited:

- The unauthorised export or transmission of school software via the internet.
- The accessing, viewing, downloading or forwarding of pornographic material or material of a racist or inflammatory nature.
- The loading, downloading or forwarding of games software.
- The generation or forwarding of messages that would be considered 'spam' e.g. chain letters.
- The sending or forwarding of abusive or offensive emails – inside or outside the school – or material that could cause offence. This applies to all email, whether intended for person-to-person communication or wider distribution.
- The use of school email for running a private business.

The list may be added to at any time. Known pornographic sites on the internet will be blocked and filters to intercept prohibited material and offensive language are in place. The school reserves the right to intercept, monitor, analyse and read all email generated, received or distributed via the school networks, equipment and email addresses.

Some email systems have the capability to send the contents of messages to fax machines. This policy applies equally to such messages and documents.

Any queries regarding this policy should be addressed to the headteacher.

Monitoring and evaluation

All use of the internet is recorded and retained for 30 days, the principal may request access to internet logs, emailing history etc if the senior management team considers that this policy has been contravened, in order to investigate alleged abuse. The policy itself will be monitored and evaluated regularly taking into account any incidents which occur or technological developments which might need a change in the policy.

APPENDIX 1

ICT: Staff acceptable computer usage agreement

I will only access the system with my own name and registered password.

Passwords that I use to access school systems will be kept secure and secret.

If I have reason to believe my password is no longer secure I will change it immediately. I will inform the network manager as soon as possible so that any access with my old password can be monitored and appropriate action taken.

I acknowledge that the computer/laptop provided for me to use remains the property of the school and should only be used for school business.

I will not access the files of others or attempt to alter the computer settings.

I will not update web logs or use pictures or text that can identify the school without the permission of the headteacher.

I will not alter, attempt to repair or interfere with the components, software or peripherals of any computer that is the property of the school.

If I use removable media I will ensure that this has been carefully checked to ensure it is free from any type of virus.

I will follow the guidance provided by ICT support staff to ensure the anti-virus protection on my laptop is kept up-to-date.

I will arrange with the network manager/technician should I need access to additional software not on the network.

I will always adhere to the following associated school policies:

- Secure data handling policy.
- ICT: staff acceptable laptop agreement.
- Staff email policy and procedures.
- Social media policy.

I will always adhere to copyright.

I will always shut down my laptop/ computer when I have finished working from it.

I understand that the school may monitor the internet sites I visit.

I understand that a criminal offence may be committed by deliberately accessing internet sites that contain certain illegal material.

I understand that staff are not permitted to access social media websites from the school's computers, staff laptop or other school device at any time unless authorised to do so by a member of the senior management team.

I will not open email attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the network manager/headteacher/ designated colleague as appropriate.

Any email messages I send will not damage the reputation of the school. All joke emails and attachments are potentially damaging and undesirable and therefore will not be used.

I will report immediately to the headteacher any unpleasant material or messages sent to me.

I will not post anonymous messages or forward spam email.

I understand that use of the school's equipment for personal financial gain, private enterprise, gambling, political purposes or advertising is forbidden.

I understand that activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.

I understand that I am responsible for the safety of sensitive school data that I use or access.

In order to maintain the security of data I will take the following steps:

I will store data files in my user area only for as long as is necessary for me to carry out my professional duties.

I will not save data files to a PC or laptop other than that provided by the school.

If I need to transfer confidential data files I will speak to the network manager/ technician.

I will not share or give out any passwords that I use to access school systems. If I have reason to believe that my password is no longer secure I will change it.

If I am in any doubt as to the sensitivity of data I am using I will refer to the school's secure data handling policy to check. Sensitive data could include:

- Pupil reports.
- SEN records.
- Letters to parents.
- Class-based assessments.
- Exam results.
- Whole school data.
- Medical information.
- Information relating to staff eg performance reviews.

I understand that if I do not adhere to these rules outlined in this agreement, my network access could be suspended, my laptop removed and that other disciplinary consequences may follow, including notification to professional bodies, where appropriate.

If an incident is considered to be an offence under the Computer Misuse Act or the Data Protection Act this may require investigation by the police and could be recorded on any future criminal record checks.

Name……

Date……..

APPENDIX 2

ICT: Staff acceptable laptop usage agreement

The laptop is the property of Tudor Park Education Trust. It has been allocated to me as a member of staff and is my responsibility. If another member of staff borrows it, the responsibility still stays with me and I understand that only school staff may use the laptop.

I understand that students must never use the laptop.

When I leave the school's employment, the laptop will be returned to the school. Should I be on extended leave of four weeks or more I will return the laptop to the school (unless I have a prior agreement with the headteacher).

I understand that when in school and not being used, the laptop must be kept in an office, locked room or drawer. It must not be left in an unlocked, unattended classroom.

I understand that, whenever possible, the laptop must not be left in an unattended.

I will check that the laptop is covered by my normal household insurance. If this is not the case, then either the insurance must be changed or the laptop should be kept in school and locked up overnight.

I understand that the laptop must not be taken abroad, other than as part of a school trip, and its use agreed by prior arrangement with the headteacher with evidence of adequate insurance.

I understand that when being transported, the carrying case supplied must be used at all times.

I understand that I should not attempt to alter the computer settings other than to personalise my desktop working area.

If any fault occurs with the laptop I will refer it immediately to the technical support staff/network manager.

I will not leave the laptop in an office or classroom during school holidays.

I will return the laptop to ICT technical support for safe keeping if do not take it home during school hoildays.

Laptop issued to _____ on _____

Staff name _____ Network support _____