Star

NURTURING TODAY'S YOUNG PEOPLE,
INSPIRING TOMORROW'S LEADERS

PUPIL ICT ACCEPTABLE USE POLICY

Document control

This document has been approved for operation within:	All Trust Schools
Date of last review	August 2018
Date of next review	August 2020
Review period	2 Years
Status	Trust Requirement
Owner	Star Academies
Version	3

Contents

Introduction

1. The School recognises the importance of ICT in education. The Internet and other digital information and communication technologies are powerful tools, which can open up new opportunities for everyone.
2. We have a range of Information and Learning Services that you will use during your time here. This is an easy to understand overview of the guidelines you need to be aware of, and comply with. This will ensure the effective running and security of the School's ICT services, and also protect you and your information.
3. This policy applies to all school computers and devices (including WiFi) and also any mobile and tablet devices that you use in school.

Aims

4. To provide you with a comprehensive Code of Conduct that clearly sets out the rules you will be expected to adhere to when using the School's ICT equipment.
5. To inform you of what you can and cannot use the School's ICT equipment for.
6. To provide guidance on how to correctly use the School's ICT equipment to save and store your work.
7. To provide information on how to effectively manage your individual user account and set your password.
8. To ensure that you use the Internet safely and responsibly.
9. To ensure that you use the School's printing facilities economically.
10. To promote E-safety throughout the School and provide advice on how to deal with matters such as cyber bullying.
11. To support the mission, vision and values of the Trust and its establishments.

Who is responsible for this policy?

12. The Trust has overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory or Trust framework. The Trust has delegated day-to-day responsibility for operating the policy to Star Central, the Local Governing Body and the Principal of each Trust school.
13. The Local Governing Body and Senior Leadership Team at each Trust school have a specific responsibility to ensure the fair application of this policy and all members of staff are responsible for supporting colleagues and ensuring its success.

Pupil accounts: setting your password

14. You will be allocated an account when joining the School which you will take responsibility for; you are responsible for all the activity that takes place under your username. Protect your login account by using a memorable password for your account. When setting your password:
    - use a combination of letters, numbers and symbols;
    - try using a memorable saying or phrase;
    - do not tell anyone your password and do not write it down.

15. If you are worried someone has guessed your account password you will need to immediately inform your class teacher and contact the ICT Department.

Pupil Accounts: saving your work

16. Your personal space on the school ICT network is known as your Z drive. Save your work to your Z: drive (My Documents) to keep it safe.
17. Do not save to the C: drive on school computers as this is not backed up.
18. If you save to a USB memory stick, make sure that you know which the most recent version is and also keep a backup copy.

Use of the internet and email

19. A web-filtering system is in place at the School. However, it is impossible to guarantee that all potentially harmful material is filtered. If you come across any inappropriate website or content whilst using the ICT equipment, you must report it to a member of staff or the ICT Department immediately.
20. The use of Internet and email is a privilege and inappropriate use will result in that privilege being withdrawn.
21. All Internet access is logged and monitored. Use of the Internet should be in accordance with the following guidelines:
    - only access suitable material – the Internet is not to be used to download, send, print, display or transmit material that would cause offence or break the law (this includes accessing sites meant for adults of 18 years or older such as pornographic or gambling sites);
    - do not access Internet chat sites - you could be placing yourself at risk;
    - never give or enter your personal information on a website, especially your home address, your mobile number or passwords;
    - do not access online gaming sites - your use of the Internet is for educational purposes only;
    - do not download or install software from the Internet, as it is considered to be vandalism of the School's ICT facilities;
    - do not use the Internet to order goods or services from online shopping or auction sites
    - do not subscribe to any newsletter, catalogue or other form of correspondence via the Internet;
    - do not download any unlicensed material such as music, videos, TV programs, games, and PDF files - this is considered illegal and therefore not permitted.
22. You will be provided with a school email account. You are expected to use email in a responsible manner.
23. Use of email should be in accordance with the following guidelines:
    - do not open or forward any email or attachment from an unrecognised source or that you suspect may contain inappropriate material or viruses - report the item to the ICT Department;
    - do not send, forward, print or transmit in any form any offensive, obscene, violent or dangerous material via email;
    - do not send or forward chain letter emails, jokes, spam etc;

- use appropriate language - what you say and do can be viewed by others;
- do not reveal any personal information about yourself or anyone else, especially home addresses, personal telephone numbers, usernames or passwords;
- consider the file size of an attachment, files exceeding 1MB in size are generally considered to be excessively large and you should consider using other methods to transfer such files.

24. If you are concerned about any email you have received, you should contact a member of staff immediately.

Use of ICT equipment

25. You have a responsibility towards the care of any school ICT equipment.
26. You must keep all liquids and food away from any ICT equipment.
27. Downloading and installing software packages on school-owned equipment is not permitted. You must not:
    - install unlicensed software on ICT equipment;
    - copy or distribute licensed software for installation on other ICT equipment;
    - deliberately port scan or use port scanning software;
    - use peer to peer file sharing software (e.g KaZaA, BearShare, Morpheus) to download or upload obscene, copyrighted or illegal material;
    - connect or attempt to connect to ICT systems without permission;
    - run server operating systems or services without permission;
    - connect any form of network device (i.e. routers, wireless access points, switches or hubs) to the ICT network;
    - deliberately or unintentionally cause the interruption of any school service or another user's data or system e.g. by virus infection;
    - save personal media images, sound or videos in the file server network.
28. You should report all faults or damage to school-owned equipment to a member of staff.
29. Vandalism to ICT equipment will result in cancellation of privileges and parents will be asked to make payments for any malicious damage to the ICT equipment. Vandalism is defined as any malicious attempt to harm or destroy data of another user and deliberately decorate or damage ICT equipment.

Social networking sites

30. You are not permitted to access social networking sites such as Facebook and Twitter in school.
31. You are not permitted to have staff at the School as contacts on social networking sites.

Printing

32. You must use printing facilities economically and only for recognised educational purposes.

Loss of data

33. The School will not be responsible for any damages you suffer. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or your errors or omissions.

Online Bullying

34. The School will not tolerate any form of bullying including electronic or online bullying. Sending or publishing offensive or untrue messages or imagery that could intimidate, harm or humiliate other pupils and their families is forbidden and could be regarded as breaking the law.
35. The School reserves the right to monitor all Internet and email activity within the bounds of current legislation in order to keep the Internet safe for all at the School and to protect from online bullies.
36. Any instances of bullying will be taken very seriously. As with any other form, cyber or online bullying will be investigated fully and will result in disciplinary action.

Hacking

37. Any type of hacking (an attempt to gain access to folders, databases, or other materials on the network to which you are not entitled) is considered to be an extremely serious offence.
38. Similarly, physical interference with another user's computer is not permitted.

Copyright

39. You must not copy or store files, documents, music, video or any other material where copyright restrictions exist, unless permission by the copyright holder has been given. Using copyright material without permission is an offence.

Sanctions

40. The following sanctions may be applied:
    - violation of the listed prohibited activities will result in a temporary or permanent ban on Internet/computer use;
    - parents/carers will be informed;
    - additional disciplinary action may be added in line with existing practise on inappropriate language or behaviour;
    - when applicable, police or the Local Authority may be involved.

Monitoring, evaluation and review

41. The policy will be promoted and implemented throughout all Trust schools.
42. The Trust will monitor the operation and effectiveness of arrangements referred to in this policy at each Trust school.
43. The Trust will review this policy every two years in consultation with each Trust school.

Summary of Acceptable Use Policy & Pupil Declaration

The following policy guidelines apply to all school computers and devices (including WiFi) and also any mobile and tablet devices that you use in school.

- DO NOT share your school account password with anyone.
- SAVE your work to Z drive.
- DO NOT access others' accounts.
- DO NOT use the Internet to:
    - access/transmit illegal or obscene material, or material that discriminates on any grounds
    - access chat or social networking sites (e.g. Facebook, Twitter)
    - access gaming sites
    - download unlicensed material such as music, videos, TV programmes etc.
    - order items from online shopping or auction sites.
- DO NOT open emails that you think may contain inappropriate material or a virus.
- DO NOT reveal any personal information about yourself online or via your email.
- DO NOT deliberately port scan or use port scanning software.
- DO NOT use peer to peer file sharing software (e.g. KaZaA, BearShare, Morpheus) to download or upload obscene, copyrighted or illegal material.
- DO NOT connect or attempt to connect to ICT systems without permission.
- DO NOT run server operating systems or services without permission.
- DO NOT make, install or distribute unauthorised copies of computer software.
- DO NOT connect any form of network device (i.e. routers, wireless access points, switches or hubs) to the ICT network.
- DO NOT copy files (images, music, video, text) that are copyright protected.
- DO NOT publish or share any information that damages the reputation of the School.
- DO NOT deliberately or unintentionally cause the interruption of any school service or another user's data or system e.g. by virus infection.
- DO NOT deliberately damage/vandalise hardware equipment in school.
- DO NOT intentionally waste limited resources, including printer ink and paper.
- DO NOT save personal media images, sound or videos in the file server network.
- DO NOT hack or physically interfere with another user's computer.
- DO NOT contact staff via social networking sites.
- DO NOT bully others online and report any bullying to a member of staff.
- REMEMBER the School may monitor your use of IT systems and online behaviour to maintain a safe school.

I have read and agree to abide by the rules stated in the ICT Acceptable Use Policy. I understand the consequences if I do not.

Name: _____ Form: _____

Signed: _____ Date: _____