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		
Status	Trust Requirement		
Owner	Star Academies		
Date effective from	July 2021	**Date of next review**	September 2024
Review period	3 Years	**Version**	5

Contents

Introduction

1. The school recognises the importance of information and communications technology (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 Wi-Fi) and also any mobile and tablet devices that you use in school.

Aims

4. To provide you with a set of 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 promote e-safety throughout the school and provide advice on how to deal with matters such as cyber bullying.
10. To support the mission, vision and values of the Trust and its establishments.

Who is responsible for this policy?

11. 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.
12. 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

13. When joining the school you are allocated an account which you take responsibility for. This account enables you to access the school provided systems (e.g., Microsoft Teams) and you are responsible for all the activity that takes place under your username. Ordinarily passwords are provided by the school, however if you are asked to set a password for your account you should:
    - use a combination of letters, numbers and symbols;
    - try using a memorable saying or phrase;
    - not tell anyone your password and never write it down.

14. If you are worried someone has guessed your account password, you will need to immediately inform a member of staff.

Pupil accounts: saving your work

15. Your personal space on the school ICT network is known as OneDrive. You should save your work to the school OneDrive unless advised otherwise by a member of staff.
16. Do not save to the C: drive on school computers as this is not backed up.
17. 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.

Pupil accounts: Microsoft Teams

18. The user login account you are provided with allows you to access school provided services such as Microsoft Teams. You are expected to use this and other services in a responsible manner, and do so in accordance with the following guidelines:
    - Do not attempt to access accounts that belong to other pupils or school staff;
    - Do not use accounts that belong to others unless permission has been granted;
    - Do not open or forward any information or attachment, or other communication from an unrecognised source or that you suspect may contain inappropriate material or viruses - report the item to a member of staff;
    - Do not send, forward, share, print or transmit - in any form - any offensive, obscene, violent, or dangerous material;
    - Do not send, forward, or share chain letter emails, jokes, spam etc;
    - Do not reveal any personal information about yourself or anyone else, especially home addresses, personal telephone numbers, usernames, or passwords;
    - Use appropriate language - what you say and do can be viewed by others;
    - Consider the file size of an attachment, files exceeding 25MB in size are generally considered to be excessively large and you should consider using other methods to transfer such files (speak to a member of staff to find out how to do this) (if allowed).
19. If you are concerned about any communication you have received, you should contact a member of staff immediately.

Use of the internet

20. A web-filtering system is in place at the school. Although internet usage is supervised and filtered within the school, it is impossible to guarantee that all potentially harmful material is filtered. Some pupils may find ways to access material that is inaccurate, defamatory, illegal or potentially offensive to some people. If you come across any inappropriate website or content whilst using the ICT equipment, you must report it to a member of staff immediately.
21. The use of the internet is a privilege and inappropriate use will result in sanctions being applied by the school.

22. All internet access is logged and monitored. Use of the internet should be in accordance with the following guidelines. You must:
    - not upload any files to social media sites; this includes images or videos that are taken on school premises;
    - 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);
    - 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;
    - not access online gaming sites - your use of the internet is for educational purposes only;
    - not download or install licenced or unlicenced software from the internet,
    - not use the internet to order goods or services from online shopping or auction sites;
    - not subscribe to any newsletter, catalogue or other form of correspondence via the internet;
    - not download any unlicensed material such as music, videos, TV programmes, games, and PDF files - this is considered illegal and therefore not permitted.

Use of ICT equipment

23. You have a responsibility towards the care of any school ICT equipment.
24. You must keep all liquids and food away from any ICT equipment.
25. Downloading and installing software packages, whether licenced or unlicenced, on school-owned equipment is not permitted.
26. You must not:
    - allow anyone to use your device when you are logged in;
    - use another user's device without their permission;
    - copy or distribute licenced software for installation on other ICT equipment;
    - deliberately port scan or use port scanning software;
    - use peer to peer file sharing software 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, and videos on the file server network.
27. You should report all faults or damage to school-owned equipment to a member of staff.
28. If the school has loaned you any ICT equipment to use at home, you must follow the same set of rules within this policy.
29. Vandalism to ICT equipment will result in sanctions 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.

30. Incidents of accidental damage will be dealt with on a case-by-case basis by the school.

Social networking sites

31. You are not permitted to access social networking sites such as Facebook, Twitter and Instagram on school equipment (either in the classroom or at home, via a loaned laptop).
32. You are not permitted to have staff at the school as contacts on social networking sites.

Loss of data

33. The school will not be responsible for any loss of data if this is caused as a result of your negligence, 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 if these rules are not followed:
    - Restricted access to the internet or computer use;
    - Additional disciplinary action may be taken in line with the Behaviour Policy;
    - When applicable, police or the Local Authority may be involved.
41. Depending on the circumstances, your parent(s)/carer(s) may be informed of any breaches of this policy.