The STAR Multi-Academy Trust

Acceptable Use Agreement – ICT and E-Technology

STAR ICT resources (including on-site systems, portable systems and those operated in the cloud such as google drive) are intended for professional educational purposes, and may only be used for legal activities consistent with the rules of the STAR Multi-Academy Trust. For the benefit of doubt all messaging possible within Trust systems are classified as email communications in this policy. This agreement is designed to ensure that all members of staff (including employees of all grades and roles, governors, trustees and volunteers using STAR systems) are aware of their professional responsibilities when using any form of ICT and related technologies such as mobile devices. Third parties having access to STAR systems should also be made aware of this policy and be expected to comply.
All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and / or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.
Members of staff should consult with their local school network manager or ICT/e-Safety coordinator for further information and clarification.

Personal Responsibility

Users are responsible for their behaviour and communications. Staff will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Policy, and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse of the network to a member of the senior leadership team.
This Policy should be read in conjunction with the: Social Media Policy, Agile Working Policy

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. All computer systems and networks including personal devices connected to STAR systems will be regularly monitored to ensure that they are being used in a responsible fashion. In the event that an employee feels there has been a breach of this policy it should be reported to their line manager or ultimately through recourse to the Trust Whistleblowing Policy.

Below is a set of rules that must be complied with. All staff:

1. Must only use the Trust provided email, internet or other related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher, CEO and Local Governing Body/Trust Board. Individual employees' internet usage and other related technologies can be monitored and logged and can be made available, on request to their line manager or Headteacher/CEO; staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation. To note, all staff gmail is held securely on google servers; the Trust reserves the right to delete or block access to emails or attachments in the interests of security. We also reserve the right not to transmit any email message
2. Must only use approved, secure email systems for school or Trust business as opposed any other email address; furthermore should staff require additional encryption/security they should discuss this with the headteacher/admin who have access to Egress email via their accounts
3. Must remember that Email messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software
4. Must not browse, download or send material that could be considered offensive, or likely to harass, inconvenience or cause needless anxiety to any other person or bring the STAR Multi-Academy Trust or any Academy within STAR into disrepute. Likewise, employees should report any accidental access of inappropriate materials or receipt of incoming messages of this nature immediately
5. Must ensure that they do not use emails or other systems to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case by case basis at the discretion of School or Trust management
6. Must ensure that all electronic communication with students and staff is compatible with their professional role
7. Must use appropriate language when using Trust systems remembering they are a representative of STAR on a global public system; no language or terminology will be tolerated which may be seen as inciting hatred or prejudice against any protected characteristic; no messages may be sent containing profanity, obscenity, slander or libel; political beliefs or commentary may not be shared using Trust systems
8. Should not use school/Trust information systems or resources (e.g. cameras, laptops, tablets or memory devices) for personal purposes without specific permission from the Headteacher or the CEO

9. Are not permitted to use personal portable media (e.g. USB stick) for storage of school or Trust related data/images without the express permission of the Headteacher/CEO
10. Should ensure that personal data (such as data held on an MIS) is kept secure and is used appropriately, whether in school, taken off school premises, or accessed remotely. Personal data can only be taken out of school when authorised by the CEO, COO, Headteacher, their delegate or Governing Body, and in line with the school's e-Safety Policy or other associated Trust policy
11. Are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, including when on external trips/visits. With the written consent of parents, the Trust permits the appropriate taking of images by staff and pupils with school equipment. It is the staff member's responsibility to establish whether such consent has been given. Children's names or other personal data should not be attached/associated with such images except with express consent, and considerable caution should be shown in allowing photographs to be taken or videos made of children participating in events such as swimming or PE, even if the school and/or students are not identified. If in doubt, contact the parent(s) and obtain specific written consent that has the photograph/image you wish to use attached, and the context in which it will be used clearly explained.
12. Should also ensure that their personal and/or professional use of social media complies fully with the Trust Social Media Policy
13. Are not permitted to contact or communicate with students, parents or conduct school business using personal email addresses or telephones, without specific permission from the Headteacher
14. Should not give out their own personal details, such as telephone/mobile number or email address, to students
15. Must not trespass into other users' files or folders unless these are officially shared with them
16. Should also ensure that use of electronic devices full complies with the Trust Agile Working Policy
17. Must ensure that all login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual other than themselves. Likewise, they must not share those of other users; if a member of staff thinks their password has been breached they must change it immediately and contact a member of the senior leadership team
18. Must ensure that they log off any network after work has finished, or lock the computer to make it secure until return; on finding any machine logged on under another's username all employees should log it off immediately
19. Must not download/install any software, system utilities or resources from the Internet or digital device without permission of the local ICT lead, network manager, headteacher or CEO, apart from that necessary to connect to the internet
20. Must not click on links in emails from un-trusted or unverified sources
21. Will support and promote STAR or any Academy within STAR e-safety and Data Security policies and help children be safe and responsible in their use of the Internet and related technologies
22. Will not send or publish material that violates the Data Protection Act or breaches the security this act requires for personal data, including data held on the Bromcom / Scholarpak / Google Apps / Office 365
23. Will not receive, send or publish material that violates copyright law. This includes materials sent / received using video Conferencing or web broadcasting technologies
24. Will ensure that any Personal Data (where the Data Protection Act applies) that is sent over the Internet will be encrypted or otherwise secured
25. Will ensure that portable ICT equipment are securely locked away when they are not being used. During transport between home and STAR or Academy or another destination equipment will not be left unattended
26. At any time and without prior notice, the STAR Multi-Academy Trust reserves the right to examine e-mail, personal file directories, and other information stored on STAR google drives, school networks or academy equipment. This examination assures compliance with internal policies, supports the performance of internal investigations, and assists with the management of STAR information systems. Permission to examine such information will only be granted by the Chief Education Officer or Chief Operations Officer

User Signature

I agree to follow this user agreement, and understand that failure to do so may result in disciplinary proceedings in line with the Trust Disciplinary Procedure. (*This form may also be completed via e-reading in google classrooms*)

Signature ……..…..… Date ……. Full Name ……..……...

School……

Appendix A (Sherburn High School)

The following is also applied to Staff at Sheburn High School:

- Need to make sure their passwords are at least 10 characters long and best practice is to follow at least 2 words that are not linked to each other, for example **1dogkennel23** or use the ThreeRandomWords technique. Passwords can be made memorable by bringing together Three Random Words such as **3redhousedogs27!**

- Should never use the following personal details for passwords:
    - Current partner's name
    - Child's name
    - Other family members' name
    - Pet's name
    - Favourite holiday
    - Something related to your favourite sports team

- Should not use the same password between different systems keeping passwords unique to individual systems.

- Staff have an account lockout policy on Domain joined machines where users have up to 10 attempts to login to their account. After 10 failed attempts, the account becomes locked for 30 minutes. Users need to contact IT Support during this time.

- Are not to move / disassemble ICT equipment.

- Have access to view / control student's screens / network sessions.

- Must not plug in mobile devices to the schools' equipment which would allow tethering (gain access to the internet).

- Understand that the school network password when changed will synchronise to their online Google and Microsoft services and override any passwords which were initially set or changed, this includes any temporary passwords which are given out and the user is required to change when next on the school network.

- Are not permitted to use public chat rooms or instant messaging services.

- Understand how to use - and don't mismanage - CC and BCC: only CC in people that really need to receive the email.

- Should be careful when replying to emails previously sent to a group or pressing the Reply All button.

- Unsubscribe from any marketing / advertisement emails that they may claim as junk.

- Are permitted to use Personal Digital Equipment, such as mobile phones and cameras to record images of students including when on external trips / visits only if they are removed / deleted from the device(s) at the earliest opportunity. With the written consent of parents (on behalf of parents) and staff, the school permits the appropriate taking of images by staff and students with School equipment. Digital images are easy to capture, reproduce and publish and therefore, misused.

- Never store / send sensitive / personal data on Laptops, Removable storage / media or email without being encrypted beforehand. ICT Support can advise and help staff if they have a requirement to take sensitive data off site be it via laptop, removable storage or email. ICT Support can even setup encryption on your devices. Recommended programs to use to encrypt data are: WinZip, 7Zip and Microsoft's BitLocker. It is possible to purchase encrypted memory sticks but these have got to be encrypted to at least a 256bit AES standard. It is up to the individual member of staff who has responsibility to inform ICT Support that their laptop, removable device or email requires encrypting for sensitive personal data.

- Should be aware that any USB storage device (memory stick / external hard drive) used in School needs to be encrypted if staff would like to write back / save back to the USB storage device otherwise the USB Storage device will remain a read only device.

- Must ensure that they save their work every 10 minutes in case of error / power cuts.