The Spire Church of England Learning Trust

School: St. John’s CE Middle School Academy

Acceptable Use Policy

General Statement

Computers and ICT equipment are provided for the benefit of all in the learning community, and to help deliver improvements in teaching and learning. Access to the facilities is a privilege and not a right. There are some basic rules that staff and learners need to follow, to ensure that everyone in our school community can benefit from these facilities.

ICT equipment

- Don't break or damage IT equipment, either on purpose or by being careless. This includes not eating or drinking near the computers.
- Please notify the ICT department of any damage to equipment or any unusual programmes in place, such as commercial software or a new web browser 'home page'.
- You should only install any software or extra hardware (printers, scanners, mice, speakers) if you have first checked with the ICT department. This is particularly important for apps, as they may have wide-ranging permissions that compromise the security of your machine and the ICT network as a whole.
- If you are connecting mobile equipment to the network, always ask ICT staff to help so that it is done safely and that your equipment can be virus checked and protected.

Security and Privacy

- Use of passwords is designed to keep your data safe online, and ensure that only you have access to your work. It also helps ICT staff track who is using resources and how they are using them.
- You should use a strong password, and must not tell anyone else what that password is.
- If someone else uses your account to break the ICT rules, and you have told them your password, you will be equally responsible for their actions.
- If you think that someone has tried to access your IT equipment or shared files inappropriately, please tell ICT immediately.
- Always lock computers and mobile devices when you are away from your desk or workspace, to prevent others accessing your files and information.
- You may have access to shared drives or shared network areas. These are provided to help collaborative working and shared research. Do not abuse these facilities to try to gain access to areas that you should not be looking at. If you find that you are able to see files and content that you don't think you should, please tell ICT staff.
- If you have access to confidential or personal information as part of your work, this must be kept only in the designated secure areas and applications.
- You must not disclose any personal information to anyone who does not have a right to see it.

Acceptable use of the Internet

- Staff and learners are encouraged to explore the internet and use a range of resources for teaching and learning. This should be done in a responsible way, and with an open-mindedness to new ideas and new ways of thinking.
- Rules about internet use apply equally to all staff and learners. This helps to promote shared values within the school, and to promote shared learning.
- Use of the internet is monitored to help ensure network security and promote efficient use of the available resources. Unusual volumes of traffic will be noted. If you are using significant internet resources you may be asked to explain how this is promotes the school's aims and values.

- Network filtering is in place to prevent access to inappropriate sites, and there is keyword logging software that flags certain terms. It will be clear to you if you have 'hit the firewall' by using a search term or location that may be inappropriate, or if your access to a site or resource is blocked. If that happens, please make a note of what you were trying to do at the time, as you may be asked to explain to a teacher or senior manager.
- Please notify ICT staff immediately if you access any inappropriate sites by accident, or if you find inappropriate content on a workstation or the internet.
- You must use the internet in accordance with UK law. Any illegal use will be dealt with through official channels, which may include the involvement of police if a crime has been committed.

The school email system

- The school provides an email system to facilitate teaching and learning. It allows staff *[and learners]* to communicate quickly with one another, and to provide a quick and easy way to deal with outside agencies on any school business.
- Anything sent through the school email system may be accessed and viewed by senior leaders if there is a valid reason to do so. The school will directly access email accounts in the course of an appropriately authorised investigation.
- Staff should not email school files or documents to personal email accounts. If you are sending a document to yourself to work on at home or at another site, use the school email address or a shared cloud server provided by the school, such as OneDrive, SharePoint or Google Drive.
- Use of email may be subject to monitoring for security and/or network management reasons.
- Your school email address should only be used for school business, and in connection with teaching and learning. It should not be used for general everyday purposes.
- Staff *[and learners]* should be aware that it is unacceptable to use the email system to send or receive any material that is obscene or defamatory, or to use it to in any way intended to annoy, harass or intimidate another person. Any reporting instances of using email in this way will be dealt with by senior leaders.

Email Security

- St. John’s CE Middle School has strong email and internet security in place. However there is always the risk that scam, phishing or chain emails may get through this, and be received on your school email account. Staff and learners need to be aware that not everything sent to your school email account may be what it seems.
- Scam or phishing emails may contain nasties such as viruses, malware and ransomware. Viruses infect your machine and make it harder to use, by example by making you unable to open programs, or changing your default internet log-in page to a scam site. Malware may track information such as your web visits and key strokes, and send this back to the scammer. This may allow them to access your online accounts. Ransomware encrypts files on your machine and locks them down. When you try to open them, you see a ransom demand to have them decrypted and returned to you.
- If you receive an unusual or suspicious email, you should not open it. You should delete it from your ‘inbox’ and your ‘delete’ box, and notify ICT staff. Do not forward suspicious emails to the ICT department. Tell ICT support basic details about the email subject and address, and allow them to investigate.

Using ICT equipment away from the school site

- You should take care when using or transporting school-issued ICT equipment away from the school site. You will be responsible for taking all due care to ensure that it is kept safe and is not lost or stolen.
- You should take additional care if working offsite to ensure that data and information on your machine is not accessed by anyone else.
- You should use your password and lock the machine if you are away from it for any length of time.
- Make sure your screen cannot be seen by other people if you are working in a public place.
- Any apps or log-ins to school systems should be closed when you are no longer using them. This will ensure that any personal data being accessed is kept safe and secure.
- Memory sticks are not secure and are easily mislaid. There are many preferable alternatives to using memory sticks to transfer and access documents away from the school site. This might include using shared cloud-drives and school email accounts for storing and accessing documents or data. If there is no alternative to using a memory stick, for example if you do not have internet access at your off-site workplace, then the memory stick must be encrypted.

What is unacceptable conduct?

- The Trust aims to encourage positive use of ICT equipment to enhance teaching and learning opportunities. Using the resources and facilities in any way that is not positive and goes against the spirit of this Policy could be considered to be unacceptable.
- All users must be aware that they must not use the school equipment or network to obtain, download, send, print, and display or otherwise transmit or gain access to materials that are unlawful, obscene or abusive or contain other objectionable materials. In addition, any kind of abuse of others is unacceptable. This would include any actions that intend to belittle others based on their race, gender, religion, sexual orientation or other aspects of their chosen social character.
- Neither staff nor learners should use the ICT facilities for commercial activities or money-making schemes. The only exception to this could relate to approved fundraising for charity; this must be signed off by senior management before any emails are sent.
- Using, uploading or downloading any commercial software or any software not approved by ICT is not acceptable. This includes using third-party browsers or VPNs to bypass internet filtering and monitoring.
- You must not try to bypass, uninstall or compromises antivirus, antimalware and anti-spyware software, and don't open any files from removable media, or from the internet, without first checking that they are free from virus or malware.

What might we monitor?

- In order to keep the network secure and available for all, and to help protect everyone in our learning community, we will monitor certain aspects of ICT and network use. This may include looking at the volume of internet, email and network traffic, logging any internet sites visited, and logging keywords that are rejected by our Firewall.
- Our school CRM package, used by staff to record information about learners and the day-to-day business of the school, has an audit function. We will use this periodically to monitor access to the system, and to ensure that it is only being used for operational reasons that enhance teaching and learning.

- The specific content of any transactions will only be monitored if there is a suspicion of improper use. If there are concerns about the way a student or learner is using the ICT facilities, this may lead to further conversations with teachers or senior managers.
- ICT staff are permitted to directly access staff *[and learner's]* email accounts if authorised by senior management, to check that they are being used appropriately. You will be told if that has occurred.

What could happen if you don't follow these rules

- These rules are intended to keep everyone in our learning community safe, and to ensure that we all benefit from the opportunities for improved and enjoyable teaching and learning that ICT can offer.
- Anyone failing to comply with these guidelines can expect further action to be taken. For staff this could include disciplinary action under the disciplinary procedure.
- If any criminal acts have taken place, then we will involve the Police as appropriate. They will have full access to all logs, back-ups and records that we hold in relation to any alleged wrong-doing.

A copy of this policy is included in the Staff Induction Pack and all new members of staff will be asked to sign to say they have seen and read this policy which will then be kept on the staff's personnel file.

Signed………………………………………………………….. Date………………………
Chair of Governors

Signed………………………………………………………….. Date……………………..

Policy review date: March 2020