THE ST. BART'S ACADEMY TRUST

Acceptable Use Policy and Remote Online learning and communication

May 2018

BTSA Britannia Teaching School Alliance

DIOCESE OF LICHFIELD GOING FOR GROWTH

National Teaching School designated by National College for Teaching & Leadership

The St. Bart's Academy Trust

Acceptable Use Policy - Learners and Staff

Produced Date:	**May 2018**
Approved by Trust Board:	**[Name]**
Review Date:	**[Date]**

Date	Section Amended	Signature

{Insert Academy Name}			
Position	**Signed**	**Print**	**Date**
Chair of Governors			
Principal			

THE ST. BART'S ACADEMY TRUST

Contents

1. 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.

2. 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 wideranging 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. Please note that if the equipment does not have anti-virus software installed then ICT staff will not add it to the network.

3. 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. On occasion, it may be necessary for you to divulge your password to ICT staff in order for them to perform maintenance, updates and install software to equipment. Passwords can be reset once completed.

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.

4. 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 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.

5. 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.

6. Email Security

St Bart's Multi-Academy Trust 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 content 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 St Barts ICT staff. If requested, please forward suspicious emails to the St Bart's team. Prior to forwarding any emails, inform the St Bart's ICT team the details of the email subject and address, and allow them to investigate.

7. 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 the schools One Drive/Goodle Drive 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.

8. What is unacceptable conduct?

St. Bart's Multi-Academy 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.

In particular, 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.

9. 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 MIS 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.

10. 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.

11. Remote Learning and online communication (AUP addition)

Guidance Notes

This addition to the policy template is provided for schools across SBMAT using remote learning, including live lessons, and other forms of online communication.

Information and guidance regarding remote learning during Covid-19:

- DfE 'Safeguarding and remote education during coronavirus (COVID-19)'
- The Education People:' Safer remote learning during Covid-19: Information for School Leaders and DSLs'
- SWGfL: Safer Remote Learning
- LGfL: Coronavirus Safeguarding Guidance
- NSPCC: Undertaking remote teaching safely
- Safer Recruitment Consortium: 'Guidance for safer working practice for those working with children and young people in education settings Addendum' April 2020

This template specifically addresses safer practice when running formal remote learning, including live streaming, but could also apply to other online communication, such as remote parent meetings or pastoral activities. However, there is no expectation that staff should run formal live streamed sessions or provide pre-recorded videos; settings should implement the approaches that best suit the needs of their community and staff following appropriate discussions.

This AUP has been completed following a thorough evaluation of remote learning tools with approval from leadership staff in each individual school. Staff in school only use approved accounts and services to communicate with learners and/or parents/carers.

Additional information and guides on specific platforms can be found at:

- https://coronavirus.lgfl.net/safeguarding
- https://swgfl.org.uk/resources/safe-remote-learning/video-conferencing-for-kids-safeguarding-and-privacy-overview/

Leadership Oversight and Approval

1. Remote learning will only take place using documents and files shared over class dojo. There are some celebratory photographic.video contact that might be shared on the school facebook page, which is for members only. School has admin control over this.
    - Class dojo has been assessed and approved by the Principal.
    - The school's facebook group page is secure.

2. Staff will only use St. Michael's managed professional email addresses/dojo log-ins with learners and/or parents/carers.

    - Use of any *personal* accounts to communicate with learners and/or parents/carers is not permitted by staff members.
        - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with Michelle Sharp, Designated Safeguarding Lead (DSL), or with David Jobling (Principal).
    - Staff will use work provided equipment *where possible* **e.g.** a school/setting laptop, tablet or other mobile device

3. Online contact with learners and/or parents/carers will not take place outside of the operating times as defined by SLT:

    - In the event of pupils needing to self-isolate at home, or of a generalised lockdown requiring a bubble or multiple bubbles to access learning remotely, online contact with pupils and parents will be during the course of the normal school hours for pupils.

4. All remote lessons will be formally agreed; a member of SLT, DSL and/or head of department is able to monitor at any time.

5. Live lessons taught through the remote sessions will only be held with approval and agreement from the Principal. In practice this will be delegated to the wider SLT, with a weekly update given at each SLT meeting.

Data Protection and Security

6. Any personal data used by staff and captured by class dojo when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.

7. All remote learning and any other online communication will take place in line with current St. Michael's confidentiality expectations as outlined in our GDPR policy.

8. All participants will be made aware that class dojo records activity. In the event of any video of photographic material that is shared over class dojo as part of home learning, staff should be clear about how recordings will be stored, how long they will be kept for and who will have access to them, in line with our existing data protection policy.

9. Staff will not record lessons or meetings using personal equipment unless agreed and risk assessed by SLT and in line with our data protection policy requirements.

10. Only members of the St. Michael's Community Academy school community will be given access to our class dojo subscription and log-ins.

11. Access to class dojo will be managed in accordance with expected safe practice, including:

    - **Strong passwords**
    - **Devices being password protected and switched off after use**
    - **Devices not being left unattended**

Session Management

12. Staff will record the length, time, date and attendance of any work done to support home learning over class dojo. This will be recorded on a standard proforma and handed in to the school office each week.

13. **It is not anticipated that live streaming will regularly take place as a routine part of the remote learning offer to children.** In the event of a live-stream being arranged, Live 1 to 1 sessions will only take place with the prior approval from the Principal or Vice-Principal and will only happen if the parent/carer is also in the room with the child.

14. If a live stream session is arranged, a pre-agreed invitation detailing the session expectations will be sent to those invited to attend. SLT will be notified in advance of any home/school interactions via live streaming.
    - **Access links should not be made public or shared by participants.**
        - Learners and/or parents/carers should not forward or share access links.
        - If learners/parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.
    - Learners are encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.

15. Alternative approaches and/or access will be provided to those who do not have access.

Behaviour Expectations

16. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.

17. All participants are expected to behave in line with existing St. Michael's policies and expectations.

This includes:

- Appropriate language will be used by all attendees.
- Staff will not take or record images for their own personal use.
- Setting decisions about if other attendees can or cannot record events for their own use, and if so, any expectations or restrictions about onward sharing.

18. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.

19. When sharing videos and/or live streaming, participants are required to:

- Wear appropriate dress.
- Ensure backgrounds of videos are neutral (blurred if possible).
- Ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.

20. Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

Policy Breaches and Reporting Concerns

21. Participants are encouraged to report concerns during remote and/or live streamed sessions:
    - Staff must report to the school Principal (David Jobling) and also log the incident in CPOMS.

22. If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to David Jobling (Principal).

23. Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour.

Sanctions for deliberate misuse may include:

- Restricted access to the school's systems
- A warning from the Principal
- Parents being asked to attend a behaviour panel meeting with a governor present
- Disciplinary action (if regarding the behaviour of a member of staff)

- The matter being reported to the police

24. Any safeguarding concerns will be reported to Michelle Sharp, Designated Safeguarding Lead, in line with our child protection policy.

I have read and understood the St. Michael's Community Academy Acceptable Use Policy (AUP) for remote learning.

Staff Member Name: ……..…….

Date…….

THE ST. BART'S ACADEMY TRUST

St. Bart's Multi-Academy Trust c/o Belgrave St. Bartholomew's Academy,

Sussex Place, Longton, Stoke-on-Trent, Staffordshire, ST3 4TP www.sbmat.org T: 01782 235524 F: 01782 235525

BTSA Britannia Teaching School Alliance

DIOCESE OF LICHFIELD GOING FOR GROWTH

National Teaching School designated by National College for Teaching & Leadership