St Christopher's Church of England High School

ICT Acceptable Use Policy

(All Staff, Supply Teachers, Visitors and Guests)

This policy applies **at all times**, in and out of directed working hours, whilst using school resources (including remote and personal connection to the school network) and equipment. The school reserves the right to withdraw access to IT resources from any staff member, visitor, and guest who behaves in an inappropriate manner or in breach of this policy.

Staff, visitors and guests must::

- ☑ Only access websites and other internet activity that is appropriate for use in school. Examples contrary to these are those pertaining to gambling websites, streaming services and retail (unless for the agreed purposes of classroom provision or resourcing). Staff should consult the Senior Network Manager wherever doubt may exist.
- ☑ Be aware that your actions on the internet are monitored and thus confidential information should not be transmitted by this medium.
- ☑ Be careful of what you communicate to others.
- ☑ Treat others, as they would expect to be treated.
- ☑ Respect copyright, trademarks and intellectual property.
- ☑ Use sensible filenames when saving your documents.
- ☑ Report any incidence of cyber-bullying or dangerous and inappropriate behaviour / content to the Designated Safeguarding Lead (DSL).
- ☑ Ensure that artificial intelligence (AI) must only be used appropriately and always in complete conjunction with the New and Emerging Technologies Policy.
- ☑ St. Christopher's staff must ensure to only use the permitted footer format. Guidance for what this should look like and how to do it are on the school SharePoint and help can be sought by emailing ICTSupport@st-christophers.org.
- ☑ St. Christopher's staff must not use any other footer, they must not embellish or adapt the footer in anyway.
- ☑ The primary form of electronic communication from a St. Christopher's staff member to a parent is via Synergy. If staff do contact parents via email they must do so from their St. Christopher's email address, should copy or blind copy their line manager into the communication and must always use professional language, signing off with their title and not their forename. Parents should be addressed in the same manner and Synergy should be consulted for the avoidance of doubt.
- ☑ Staff must be mindful that any form of written communication which is digital and unencrypted, whether via email or Microsoft Teams is the property of St. Christopher's and may also be requested as evidence in a subject access request (SAR).

Staff, visitors, and guests must not:

- ☒ Tell anyone else your password or log on to the network using someone else's password.
- ☒ Send, access or display offensive messages or pictures, or use inappropriate language.
- ☒ Use the school's IT facilities for sending personal e-mails, the completion of subscription forms or the conduct of monetary business.
- ☒ Take photographs or video of staff, pupils or students without prior permission.
- ☒ Publish on the internet (incl. Facebook or any other social media platforms) material such as text, videos or photographs of staff or pupils without prior permission. This includes using your own resources.
- ☒ Use the school's IT facilities to post anonymous messages, or forward chain messages or access chat programs without permission.
- ☒ Use a USB stick or drive at any time.
- ☒ Save or install MP3, video files, games or third-party programs to the school network.
- ☒ Access any inappropriate websites, or view unsuitable images or videos.
- ☒ Access websites that encourage vandalism, crime, terrorism, racism, eating disorders or suicide.
- ☒ Attempt to circumnavigate the proxy and security systems that are in place.
- ☒ Staff members are strongly advised not to communicate directly with pupils and students. In the event that a member of staff must contact a student or pupil it must be from a St. Christopher's email address to the pupil or student's St. Christopher's email address and the head of department should be copied or blind copied in

Please note:

- User-areas on the school network will be closely monitored and key staff may review your files and communications to maintain system integrity.
- Websites that are accessed by pupils are recorded and checked regularly to ensure that all pupils, staff and visitors are safe and adhering to the school's Internet policy.
- If you access an unsuitable website by accident or encounter any material that makes you feel uncomfortable, you should notify key staff.
- Failure to follow the school's ICT Acceptable Use Policy will result in loss of access and further disciplinary action may be taken, if appropriate. If applicable, external agencies such as the Police may be involved, as certain activities may constitute a criminal offence.

Key Staff:

In addition to the Headteacher:

Mr D. Pilkington - Senior Network Manager

Mr D. Allen - Assistant Headteacher Responsible for New and Emerging Technologies)

Mrs L. Williamson - Designated Safeguarding Lead).