The login AUP:

In order to safeguard students and colleagues it is important that all staff take all possible measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All colleagues have a responsibility to use the school's computer system in a professional, lawful and ethical manner.

- School owned information systems must be used appropriately. I understand that the Computer Misuse Act, 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I understand that any hardware and software provided by the school for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password - one that contains letters (upper and lower case), numbers and possibly symbols which I will change on a regular basis. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
- I will ensure that any personal data of students, staff or parents is kept in accordance with the Data Protection Act, 1988.
- I will not keep professional documents which contain school related sensitive or personal information (including images, files or videos) on any personal devices unless they are secured and encrypted.
- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
- I will respect copyright and intellectual property rights.
- I have read and understood the school e-safety policy.
- I will report all incidents of concern to the DSL and/or a member of SLT.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. I will report all suspected computer system damage, of virus or other malware to the IT support.
- My communications with students, parents and other professionals will only take place via work approved communication channels. Any pre-existing relationships which may compromise this will be discussed with the Headteacher
- I will promote e-safety with students and help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- I understand that my use of the school information systems, internet and email may be monitored.

September 2019.

St Benedict's Catholic High School, Kinwarton Road, Alcester, Warwickshire B49 6PX
Tel: 01789 762888 - Email: admin@st-benedicts.org - Website: www.st-benedicts.org
Headteacher: Mr D Hughes

A member of the Holy Family Catholic Multi-Academy Company Registered in England and Wales, No. 10657219
c/o St. Benedict's Catholic High School, Kinwarton Road, Alcester B49 6PX