

# IT and e-safety use policy

## Acceptable Use Policy – ICT

- Transmission of any material in violation of any U.K. laws is prohibited. This includes, but is not limited to, copyright material, threatening or obscene materials (as determined by the Principal).
  - Use for personal commercial activity or advertising of any kind or nature or political or political lobbying is strictly prohibited.
  - The personal address, e-mail address or telephone number of students or staff must not be revealed without the user's express permissions (except by authorised persons in connection with a criminal investigation).
  - All communications and information accessible via the network should be assumed to be private property.
  - The school uses software to monitor all ICT systems for safeguarding purposes.
  - The network must not be abused or used in a manner that would disrupt the use of the network by other users.
  - Security on any computer system is a high priority, especially when the system involves many users. Users may not use another individual's account without written permission from that individual and the Network Manager.
  - Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet or any of the agencies or other networks that are connected to the Internet. This includes, but is not limited to, the uploading or creation of computer viruses.
  - Connection of file storage devices (memory sticks, standalone drives, iPods, mobile phones etc.) to the network is only allowed with the permission of the Network Manager. Any infection damage caused, whether deliberate or accidental, may be considered to be vandalism.
  - Attempts to log on as a system administrator are specifically denied. Any such attempts will result in cancellation of the user's privileges.
  - Any user sending inappropriate messages to any other person may be barred from e-mail access and may be denied access to other parts of the network.
  - Taking photos or videos of other students or staff without their permission, or broadcasting them on the internet is not permitted.
- All users accept that LST may check users' files and monitor Internet sites visited by users in support of this Acceptable Use Policy.

Failure to comply with this Acceptable Use Policy may result in the withdrawal of access to the ICT systems and other sanctions under the Academy's Student Engagement Policy or Staff Discipline Policy and associated procedures.

e-safety code\*

- I promise to tell a member of staff if I read or see something whilst using a computer or tablet that is inappropriate or makes me feel uncomfortable.
- I will not give any personal information to anyone online such as my last name, address, phone number or that name and address of my school without my teacher's permission.
- I will only use appropriately rated software and applications.
- I will not use computers or tablets to bully or abuse others.
- I will only use camera and audio recording functions when permitted to do so and I will not use in social time unless I have permission to do so.
- I will not publish photographs from within the Academy to any online network.

\* This does not replace or supersede any e-safety policy or linked policy but is meant as guidance on how to be e-safe.