Canonium Learning Trust

E-Safety Policy

Adopted: 2019/2020 *Next review: 2022/2023*

The following policy addresses the issue of Internet Safety. It is to ensure that every child in our care is safe, and the same principles apply to the 'virtual' or 'digital' world as would be applied to the Trust academies' physical buildings. This Policy protects all parties: the pupils, the staff and the Trust academies. It provides clear advice and guidance on how to minimise risks and how to deal with any infringements.

The technologies

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, we build in the use of these technologies throughout the curriculum in order to arm our young people with the skills to access life-long learning and employment.

Current and emerging Internet and online technologies used in schools (examples shown below) and, more importantly in many cases, used outside of school by children include:

- Websites (through individual searches or direct link activities)
- Learning Platforms and Virtual Learning Environments (for example MyMaths and PurpleMash)
- E-mail and Instant Messaging (2email, WordPress, Skype)
- Chat Rooms and Social Networking *(not available in school)*
- Blogs and Wikis (WordPress)
- Podcasting (iMovie)
- Video Broadcasting (School Blog and iMovie)
- Music Downloading *(not available in school)*
- Gaming *(not available in school)*
- Mobile/ Smart phones with text, video and/ or web functionality *(not available in school)*
- Other mobile devices with web functionality *(iPads/Laptops)*
- Livestreaming of video and audio

Teaching safe use of the Internet and ICT

Whilst exciting and beneficial both in and out of the context of education, policing of its use continues to be challenging. In school, our users are taught (at least yearly) an awareness of the range of risks associated with the use of these technologies and what to do to minimise them.

To maintain our pupils security and confidence when accessing and using ICT the children are consistently taught to follow the Essex modelled eSafety rules (goo.gl/vSXb5k Pg 9) in particular points 6-9. This is alongside an annual safety week where the topic is covered in depth. *Points 6 – 9 listed below:*

6 • I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.

7 • I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately.

8 • I will not give out my own details such as my name, phone number or home address.

9 • I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.

The academy will also provide a means of confidentially reporting concerns through an icon on its webpage.

Blog Publishing Management

- The class teacher will ensure all blog posts are relevant to the children's learning and are appropriate to the readers.
- The point of contact on the web site should be the school address and telephone number. Home information or individual e-mail identities will not be published
- **Children, whose parents have not granted permission to use their photograph, cannot appear on the blog.**
- First names OR photographs may be posted but not both together. **Children should not be individually identifiable through the blog.**
- Video footage of the children will be hosted on the school webpage, and is not linked externally.

Livestreaming

At times, the school will use video livestreaming services to provide content and teaching for its pupils and parents. The school will act as a host for such services. Staff should only join another's stream if express permission is given by the SLT.

- The organiser will only use the school accounts to provide this service.
- The stream will not be recorded and chat functions will only be enabled where an adult can actively monitor them. **File sharing will not be allowed during these sessions.**
- The stream will only happen during normal school hours and there will be at least two supervising staff members involved in the stream.
- On public streams, the school will follow the same guidelines as it uses for Blog Publishing (above).
- For private streams (Zoom, Skype, Google Hangouts etc.) logon credentials will be provided through the school's current secure parent contact method (ParentMail, ParentPay) and not publicly.

Children and parents will be given guidance on how to use the services to ensure the greatest accessibility and safety (see **Teaching safe use of the Internet and ICT** above). A link can be found on the Academy's website and the Canonium Learning Trust's website.

Authorisation of Internet Access

- All parents are asked to sign a form allowing their children to use the internet as part of their learning on school property. The form goes out to the parents of children in Reception and is valid for the duration of their time in the school.

Risk Assessment

- RM (Our ISP – Internet Service Provider) use a sophisticated content filter to ensure that as far as possible, only appropriate content from the Internet finds it way into school. Whilst this filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter. Children are taught what to do if they come across something unfamiliar or threatening (minimising not deleting content, telling a trusted adult directly, using report functions), so that they can do this at school as well as at home.
- The school will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a terminal. Neither the school, nor Essex County Council can accept liability for the material accessed, or any consequences thereof.
- The school actively seeks the latest information and technology to support safe access to the internet through internal CPD and through advice from external suppliers/government guidance.
- The school has a duty of care to protect the electronic data it holds on its own premises and on cloud-based services. All school laptops have appropriate anti-virus software and staff are advised to not use personal devices to access school data. Staff are required to use suitable passwords to protect remote access services (like email) and, where possible, this includes two-factor authentication.
- The school can use VPNs (virtual private networks) to allow access to the school remotely as if the user was on-site. To prevent this provision from putting confidential data at risk, only senior staff

members will have access to this service and they will be provided with guidance on how to use this service securely (i.e. password security, the devices that can used etc.).

Staff Guidance (taken from the Code of Conduct Policy– please refer to policy for further guidance)

Access to Social Networking Sites

The following permissions are given in respect of social networking applications:

- A Complete block from personal use on all school devices but restricted personal use eg during lunch hour and after work on personal devices only if used out of sight of pupils (staffroom).
- School devices can be used by staff, with pupils on approved social networking sites (Blogs).
- Personal devices should never be used with or by pupils.

Use of Mobile Telephones

- Employees are required to ensure mobile telephones are switched off/to silent during working hours and accessed only during authorised breaks. Employees are not permitted to use their mobile telephones except in the staff room unless before 8.30am or after 4.30pm.
- Any urgent phone calls or messages must be directed to the office who will notify employees immediately. Employees who need to use their mobile telephone to make or receive an urgent call during working hours should where possible obtain prior authorisation from the Headteacher.
- Employees are not permitted to contact pupils by telephone, text message or by sending picture messages using their mobile telephone or divulge their telephone number to pupils under any circumstances.
- Employees provided with a mobile telephone to carry out their duties must ensure they only use the mobile telephone for the purposes agreed. Any unauthorised usage must be reimbursed to the school.

Password policy

The trust recognises that all passwords are fallible and that no system is 100% secure. It also recognises that many current practises (like including special characters and requiring a new password within a timeframe) can be detrimental to security (https://www.ncsc.gov.uk/collection/passwords/updating-your-approach). Therefore, it requires all staff use a password that follows the following guidelines.

- Does use a separate password for remote services (email) and local services (windows logon, SIMS)
- Does use three unrelated words that have a significant meaning to the user
- Does have a minimum of 8 characters.

- Does not replace letters for characters i.e. a as 4, I as 1
- Does not use personal information i.e. names, places or a link to the school. *A full-suggested list is found at https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/use-a-strong-and-separate-password-for-email.*
- Does not get used for non-school related logins

Where needed, further guidance will be provided for individuals on best practise. For some key staff this might include the use of a password manager to provide a secure database for multiple passwords.