Information and Communication Technology Policy

ICT in the curriculum

ICT is a crucial component of every academic subject and is also taught. The School's classrooms are equipped with projectors and computers. There is a wi-fi connection available for students everywhere which is monitored in the same way as computer terminals.

Students at CERENE are taught how to research on the internet and to evaluate sources. They are educated into the importance of evaluating the intellectual integrity of different websites and why some apparently authoritative sites need to be treated with caution.

The role of technology in our students' lives

The existing communications revolution gives young people unrivalled opportunities. It also brings risks. It is an important part of the School's role to teach students how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, bullying, harassment, grooming, stalking and abuse. They also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment.

Role of CERENE

With the explosion in technology, the School recognises that blocking and barring sites is not sufficient. CERENE needs to teach all of its students to understand why they need to behave responsibly if they are to protect themselves. This aspect is a role for all the School's staff. The school has a key role in maintaining a safe technical infrastructure and in keeping abreast with the rapid succession of technical developments. The school ensures the security of the hardware system, its data integrity and trains the staff in the use of ICT. The use of the internet is monitored and inappropriate usage is immediately dealt with by the Head of School.

Role of our Designated Safeguarding Leaders

The School recognises that internet safety is a child protection and general safeguarding issue.

Staff has been trained in the safety issues involved with the misuse of the internet

and other mobile electronic devices. They work closely with the School's DSLs who, in turn, work with the Local Safeguarding Children Board (LSCB) and other agencies in promoting a culture of responsible use of technology that is consistent with the ethos of CERENE. All staff has also received training in e-safety issues. The DSL will ensure that all year groups in the secondary section are educated on e-safety issues, in the risks and the reasons why they need to behave responsibly online. It is his responsibility to handle allegations of misuse of the internet.

In the Primary section, classroom teachers are responsible for their students' e-safety.

Misuse: statement of policy

CERENE will not tolerate any illegal material and will always report illegal activity to the police and/or the LSCB. If the School discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). The School will impose a range of sanctions on any student who misuses technology to bully, harass or abuse another student in line with our anti-bullying policy.

Involvement with parents and carers and guardians

CERENE seeks to work closely with parents and carers in promoting a culture of e-safety. The School will always contact parents and carers if it has any concerns about students' behaviour in this area and likewise it hopes that parents and carers will feel able to share any concerns with the School. The School recognises that not all parents and carers may feel equipped to protect their son or daughter when they use electronic equipment at home. The School arranges discussions for parents and carers when an outside specialist advises about the potential hazards of this expanding technology and the practical steps that parents and carers can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity.

Charter for the safe use of the internet and electronic devices

E-safety is a whole school responsibility and CERENE students have adopted and signed a computer user agreement for the safe use of the internet inside the School. CERENE expects all students to adhere to the computer agreement. Copies are given to all students and their parents, and the School may impose sanctions for the misuse, or attempted misuse of the internet, mobile phones and other electronic devices.

Cyberbullying

- Cyberbullying is a particularly pernicious form of bullying because it can be so pervasive and anonymous. There can be no safe haven for the victim who can be targeted at any time or place. The School's Anti-Bullying Policy describes the preventative measures and the procedures that will be followed when the School discovers cases of bullying.
- Proper supervision of students plays an important part in creating a safe ICT environment at school but everyone needs to learn how to stay safe outside

the School.
- CERENE values all of its students equally. It is part of the ethos of the school to promote considerate behaviour and to value diversity.
- Bullying and harassment in any form should always be reported to a member of staff. It is never the victim's fault, and he or she should not be afraid to come forward.

Treating other users with respect

- The School expects students to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face-to-face contact. All students agree to obey certain rules and obligations; in particular they undertake not to harass or cyber bully others or publish photos without the consent of the person concerned. The School expects a degree of formality in communications between staff and students and would not normally expect them to communicate with each other by text or mobile phones. Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. The School's Anti-Bullying Policy is published on the School's website. The School is strongly committed to promoting equal opportunities for all, regardless of race, gender, gender orientation or physical disability.
- All students are encouraged to look after each other and to report any concerns about the misuse of technology or a worrying issue to a member of staff.

Keeping the school network safe

- The School adheres to best practice regarding e-teaching and the internet.
- Certain sites are blocked by the School's filtering system and students' use of the network is monitored.
  The School issues all students with their own personal school email address. Access is via personal LOGIN, which is password protected. The School gives guidance on the reasons for always logging off and for keeping all passwords securely.
- Access to social networks site is not allowed on school networks and is blocked.
- The School has strong anti-virus protection on its network
- Any member of staff or student who wishes to connect a removable device to the School's network is asked to arrange in advance to check it for viruses and to ensure compliance with the School's data encryption policy.

Promoting safe use of technology

students of all ages are encouraged to make use of the excellent online resources that are available from sites such as:

- UK Council for Child Internet Safety (http://www.education.gov.uk/ukccis)
- Childnet International (www.childnet-int.org)
- Cyber Mentors (www.cybermentors.org.uk)
- Cyberbullying (www.cyberbullying.org)
- E-Victims (www.e-victims.org)
- Bullying UK (www.bullying.co.uk)

E-safety is discussed during assemblies.

Safe use of personal electronic equipment

- The School's guidance is that students and staff should always think carefully before they post any information online. Content posted should not be inappropriate or offensive, or likely to cause embarrassment to the individual or others.
- The School offers guidance on the safe use of social networking sites and cyberbullying.
- The School's lessons include guidance on how students can identify the signs of a cyber-stalker and what they should do if they are worried about being harassed or stalked online.
- The School offers guidance on keeping names, addresses, passwords, mobile phone numbers and other personal details safe. Privacy is essential in the e-world.
- The School gives guidance on how to keep safe at home by encrypting the home wireless network, not opening unknown attachments and reporting any illegal content.
- Similarly the School covers how a mobile phone filter can be activated and how to block nuisance callers.
- The use of a VPN on the computer is strictly prohibited. The School will conduct random checks and students having the VPN (Virtual Private Network) installed will be severely sanctioned.

Mobile phones and other electronic devices

Mobile phones and other personal electronic devices are switched off and left with an administration officer during the entire time spent at school. Sanctions may be imposed on students who do not respect the rule.

Date: July 2016

Review: July 2017