Castle Donington College

ICT/E-Safety Policy

Date agreed by Full Governing Board **4th March 2019**

Date for review **March 2020**

Signed by Chair of Governors

The College follows Guidance and Advice given by the Government and Local Authority when writing policies; in light of this, changes may need to be made after the adoption of this policy and prior to the review date.

Introduction

Castle Donington College recognises that the internet and other digital technologies have an essential role to play in children's education. These technologies allow all those involved in the education of students to promote creativity, stimulate awareness and enhance learning.

As part of our commitment to learning and achievement, we at Castle Donington College want to ensure that technologies are used to:

- Raise standards
- Develop the curriculum and make learning exciting and purposeful
- Enable students to learn in a way that ensures their safety and security
- Enhance and enrich their lives and understanding

This policy document is drawn up to protect all parties – the students and the staff and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements. It applies to: all students, teaching and support staff (including peripatetic), College Governors and volunteers; all aspects of the College's facilities where they are used by voluntary, statutory or community organisations.

Scope of Policy

We are committed to ensuring that all students will be able to use the technologies safely. We are committed to ensuring that all those who work with students, as well as their parents/carers, are informed about the risks that exist so that they can take an active part in safeguarding against risks such as exploitation, radicalisation and bullying and discrimination. Other dangers include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Access to unsuitable video / Internet games
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files

Many of these risks reflect situations in the off-line world and it is essential that this E-Safety policy is used in conjunction with other College policies (e.g. Behaviour and Exclusions, Anti-Bullying and Safeguarding/Child Protection policies).

Policy Statements

Education - Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in E-Safety is therefore an essential part of the College's –Safety provision. Children and young people need the help and support of the College to recognise and avoid –Safety risks and build their resilience.

- Staff reinforce E-Safety messages across the curriculum. The College's E-Safety curriculum is broad, relevant and provides progression, with opportunities for creative activities in the following ways
- A planned E-Safety curriculum is provided as part of PSHEE /other lessons and is regularly visited
- Key E-Safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students are taught to be crucially aware of the content they access on-line and be guided to validate the accuracy of information
- Students are encouraged to adopt safe and responsible use both within and outside College
- Staff act as good role models in their use of digital technologies, the Internet and mobile devices
- Where students are allowed to freely search the Internet, staff are vigilant in monitoring the content of the websites visited
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in Internet searches being blocked. In such a situation, staff request that the Network Manager temporarily remove those sites from the filtered list for the period of study. Any request to do so, is auditable, with clear reasons for the need.

Education – parents/carers

Parents and carers play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Parents need to be aware of how often children and young people come across potentially harmful and inappropriate material on the Internet and maybe unsure of how to respond.

The College will provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website
- Parents'/Carers' evenings
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant websites/publications

Education & Training – Staff/Volunteers/Governors

It is essential that all staff received E-Safety training and understand their responsibilities, as outlined in this Policy. Training will be offered as follows:

- A programme of E-Safety training will be made available for staff. This will be regularly updated
- All new staff receive E-Safety training as part of their induction programme, ensuring that they fully understand the relevant College policies
- SLT will provide advice, guidance and training to individuals as required

Technical – infrastructure, equipment, filtering and monitoring

The technologies involved.

IT in the modern world has an all-encompassing role within the lives of children and adults. New technologies are changing the way we communicate and share information. Current and emerging technologies used by children and adults include but are not limited to the below:

- Email
- Social Media/Instant messaging
- Blogs
- Podcasting
- Video broadcasting sites
- Chat Rooms
- Gaming Sites
- Music download and streaming sites (Popular
- Smart phones with camera, e-mail, web functionality, instant access to social networks and video conferencing).
- Other technical devices

The College is responsible for ensuring that the College network is as safe and secure as is reasonably possible and that procedures detailed within this Policy are implemented.

- There will be regular reviews and audits of the safety and security of College technical systems
- Servers, wireless systems and cabling are securely located and physical access restricted
- All users will have clearly defined access rights to College technical systems and devices
- All users will be provided with a username and secure password – an up to date record of users and their usernames will be recorded. Users are responsible for the security of their username and password and will be required to change their password every time when prompted

- The 'administrator' passwords for the College IT system, used by the Network Manager will be available for the Principal or other nominated senior leader and kept in a secure place
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Content lists are regularly updated and Internet use is logged and regularly monitored
- There is a clear process in place to deal with requests for filtering changes
- The College has provided differentiated user-level filtering (allowing different filtering levels for different groups of users – staff/students etc)
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the College systems and data. The College infrastructure and individual workstations are protected by up to date virus software
- The use of removable media is prohibited for students. Staff may only use encrypted drives.
- There is web logging software in place, which monitors and records anything the students do online and in class. Anything not appropriate is flagged up and reports to the Network Manager

Data Protection

Staff ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged off' at the end of any session in which they are using personal data
- Transfer data using encryption and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with College policy once it has been transferred or its use is complete

Social Media – Protecting Professional identity

The College has a separate Staff Social Media Policy.

Social Media and e-Safety

The use of Social Media by students at home often intrudes on College life, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary sanctions for inappropriate

behaviour. This is pertinent to incidents of cyber-bullying or other e-Safety incidents covered by this policy, which may take place out of College, but is linked to membership of the College. The majority of these issues are linked to Social Media use.

The College expects that students will continue to show respect to other members of the College community when off site. To clarify this point:

- Students should not bully, intimidate, abuse, harass or threaten other members of the College community
- Students should not post content that is hateful, threatening, pornographic or incites violence against others
- Students should not impersonate or falsely represents other members of the College community
- Students are expected to show respect to the good reputation to the College and its staff
- Students should not film, record or photograph members of the College community without their express permission, and that of the College

The College's Behaviour and Exclusions Policy states that devices can be confiscated and searched if the College believes the images or recordings could be used to do harm.

How will complaints regarding e-Safety be handled?

The College will take all reasonable precautions to ensure E-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a College computer or mobile device. The College therefore cannot accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions.

Sanctions available include:

- interview / counselling by tutor / those with pastoral responsibility / Network Manager or a member of senior staff
- informing parents or carers
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework]

Complaints of cyberbullying are dealt with in accordance with a College's Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with the College's Safeguarding and Child Protection procedures.

It is more likely that the College will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible

in a proportionate manner, and that members of the College community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour and disciplinary procedures.

Parents and carers will be encouraged to support the College in promoting good E-Safety practice and to following guidelines on the appropriate use of:

- Digital and video images taken at College events
- Access to parents' sections of the website and on-line student records
- Their children's personal devices in the College (where this is allowed)