# Castle Donington College

# E Safety Policy

**Date agreed by the Full Governing Board** **7th July 2020**

**Date for review** **July 2023**

**Signed by Chair of Governors**

***This College follows Guidance and Advice given by the Local Authority and Government 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.***

## Contents

## 1. Aims

Castle Donington College aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole College community in its use of technology
- Establish clear mechanisms to identify, intervene in and escalate an incident, where appropriate

## 2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for Colleges on:

Teaching online safety in Colleges

Preventing and tackling bullying and cyber-bullying: advice for Principals and College staff

Relationships and sex education

Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

## 3. Roles and responsibilities

### 3.1 The Governing Board

The Governing Board has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The Governing Board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the College's ICT systems and the internet (appendix 3)

### 3.2 The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the College.

### 3.3 The Designated Safeguarding Lead

Details of the College's DSL and deputy/DSL Team are set out in our Child Protection and Safeguarding Policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety in College, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the College
- Working with the Principal, ICT Manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on CPOMS and dealt with appropriately in line with the College Behaviour Policy
- Updating and delivering staff training on online safety (Appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in College to the Principal and/or Governing Board

This list is not intended to be exhaustive.

### 3.4 The ICT Manager

The ICT Manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at College, including terrorist and extremist material
- Ensuring that the College's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the College's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are passed to the DSL, logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the College Behaviour Policy

This list is not intended to be exhaustive.

### 3.5 All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the College's ICT systems and the internet (Appendix 2), and ensuring that pupils follow the College's terms on acceptable use (Appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the College Behaviour Policy

This list is not intended to be exhaustive.

### 3.6 Parents

Parents are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the College's ICT systems and internet (Appendix A)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

### 3.7 Visitors and members of the community

Visitors and members of the community who use the College's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix B).

## 4. Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum.

Castle Donington College Computing Curriculum reflects the National Curriculum computing programmes of study.
From September 2020, Castle Donington College will teach:
Relationships and sex education and health education

This new requirement includes aspects about online safety and Castle Donington College is following the RSE 2020 guidance.

**Key Stage 3 Curriculum**

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

**Key Stage 4 Curriculum**

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of a pupil's time at Castle Donington College**, they will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including prison sentences
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

The safe use of social media and the internet will also be covered in other subjects where relevant.

Castle Donington College will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

## 5. Educating Parents about Online Safety

The College will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety advice and support will also available at parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL.

Concerns or queries about this policy can be raised with the Principal.

# 6. Cyber-bullying

## 6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the College Behaviour Policy.)

## 6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others.

We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The College will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form Tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

Castle Donington College also makes information on cyber-bullying available to parents on the website and through the Phoenix Newsletter so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the College will follow the processes set out in the College Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the College will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the Police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

## 6.3 Examining Electronic Devices

College staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the College rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of College discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the College complaints procedure.

## 7. Acceptable Use of the Internet in College

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the College's ICT systems and the internet (Appendices A and B). Visitors will be expected to read and agree to the College's terms on acceptable use if relevant.

Use of the College's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the Acceptable Use Agreement in Appendix B

## 8. Pupils Using Mobile Devices in the College

Acceptable use of mobile phones and electronic devices for pupils is set out in the College Mobile Phone/Electronic Devices Policy

Any use of mobile devices in College by pupils must be in line with the Mobile Phone/Electronic Devices Policy and the Acceptable Use Agreement (see Appendices A and B).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the College Behaviour Policy, which may result in the confiscation of their device.

## 9. Staff Using Work Devices Outside the College

Staff members using a work device outside College must not install any unauthorised software on the device and must not use the device in any way which would violate the College's terms of acceptable use, as set out in Appendix B.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside College. Any USB devices containing data relating to the College must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT Manager.

Work devices must be used solely for work activities.

## 10. How the College will respond to issues of misuse

Where a pupil misuses the College's ICT systems or internet, we will follow the procedures set out in our Behaviour Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the College's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/Staff Code Of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The College will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the Police.

## 11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and DSL Team will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

## 12. Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every three years by the Principal. At every review, the policy will be shared with the Governing Board.

## 13. Links with other policies

This online safety policy is linked to our:

Child Protection and Safeguarding Policy
Behaviour Policy
Staff Disciplinary Procedures
Data Protection Policy and Privacy Notices
Complaints Procedure
ICT and Internet Acceptable Use Policy

## Appendix A: Acceptable Use Agreement (pupils and parents/carers)

| ACCEPTABLE USE OF CASTLE DONINGOTN COLLEGE'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS | |
|---|---|
| **Name of pupil:** | |
| **I will read and follow the rules in the acceptable use agreement policy**<br>**When I use the College's ICT systems (like computers) and get onto the internet in College I will:**<br>• Always use the College's ICT systems and the internet responsibly and for educational purposes only<br>• Only use them when a teacher is present, or with a teacher's permission<br>• Keep my username and passwords safe and not share these with others<br>• Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer<br>• Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others<br>• Always log off or shut down a computer when I'm finished working on it<br><br>**I will not:**<br>• Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity<br>• Open any attachments in emails, or follow any links in emails, without first checking with a teacher<br>• Use any inappropriate language when communicating online, including in emails<br>• Log in to the College's network using someone else's details<br>• Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision<br><br>**If I bring a personal mobile phone or other personal electronic device into the College:**<br>• I will not use it during the day and it will remain switched off (see Pupil's Mobile phone/ electronic Devices Policy)<br>• With permission, I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online<br><br>**I agree that the College will monitor the websites I visit and that there will be consequences if I do not follow the rules.** | |
| **Signed (pupil):** | **Date:** |
| **Parent/carer's agreement:** I agree that my child can use the College's ICT systems and internet when appropriately supervised by a member of College staff. I agree to the conditions set out above for pupils using the College's ICT systems and internet, and for using personal electronic devices in the College, and will make sure my child understands these. | |
| **Signed (parent/carer):** | **Date:** |

## Appendix B: acceptable use agreement (staff, governors, volunteers and visitors)

| ACCEPTABLE USE OF THE COLLEGE'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS | |
|---|---|
| **Name of staff member/governor/volunteer/visitor:** | |
| **When using the College's ICT systems and accessing the internet in the College, or outside the College on a work device (if applicable), I will not:**<br>• Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)<br>• Use them in any way which could harm the College's reputation<br>• Access social networking sites or chat rooms<br>• Use any improper language when communicating online, including in emails or other messaging services<br>• Install any unauthorised software, or connect unauthorised hardware or devices to the College's network<br>• Share my password with others or log in to the College's network using someone else's details<br>• Take photographs of pupils without checking with teachers first<br>• Share confidential information about the College, its pupils or staff, or other members of the community<br>• Access, modify or share data I'm not authorised to access, modify or share<br>• Promote private businesses, unless that business is directly related to the College | |
| • I will only use the College's ICT systems and access the internet in the College, or outside the College on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.<br>• I agree that the College will monitor the websites I visit and my use of the College's ICT facilities and systems.<br>• I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside the College, and keep all data securely stored in accordance with this policy and the College's data protection policy.<br>• I will let the designated safeguarding lead (DSL) and ICT Manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.<br>• I will always use the College's ICT systems and internet responsibly, and ensure that pupils in my care do so too. | |
| **Signed (staff member/governor/volunteer/visitor):** | **Date:** |