CAISTOR GRAMMAR SCHOOL
ONLINE SAFETY POLICY

Approved by Full Governing Body on 20 May 2019…….

Reviewed… …….

Signed……..

Chair of Governors

Contents

1. Aims

Our school aims to:

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

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education (2018), and its advice for schools on preventing and tackling bullying and 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 students' electronic devices where they believe there is a 'good reason' to do so.

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 headteacher 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). The governor who oversees online safety is Andrew Gibson.

All governors will:

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

3.2 The Headmaster

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

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, IT network manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy (via CFC or in the Safeguarding folder)
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately (in some cases by the HoS) in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Liaising with the pastoral administrator who monitors Causes for Concern

This list is not intended to be exhaustive.

3.4 The IT Network Manager

The IT Network Manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any incidents of cyber-bullying that are reported are communicated to the Deputy Head appropriately in line with the school behaviour policy
- Makes staff and students aware of any 'scam' emails
- Restricts access for individual IT users as directed by the Headmaster/ Deputy Head.

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 school's ICT systems and the internet and ensuring that students follow the school's terms on acceptable use, which are published to students in their planners and highlighted to parents
- 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 school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

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

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

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

4. Educating students about online safety

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

Students in **Key Stage 3**, students 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
-

Students 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

The safe use of social media and the internet will also be covered in other subjects where relevant. The school will use PSHE and assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

5. Educating parents about online safety
The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website's Be Aware section. This policy is also published on our website.

If parents have any queries or concerns in relation to the school's online safety policy, these should be raised in the first instance with the Headmaster.

The School has a Wi-Fi network which is available to all students but it is acknowledged that 3G and 4G networks offer better access around the school site. Parents are encouraged to implement appropriate filtering devices with the student's mobile network provider. The School endeavours to inform parents of support available via the School website, on our 'Be Aware' page and via the Headmaster's weekly newsletter.

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 school behaviour policy.)

6.2 Preventing and addressing cyber-bullying
To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form teachers 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 students are made aware of cyber bullying, its impact and ways to support children as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents 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 school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The Headmaster 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
School 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 students' electronic devices, including mobile phones, iPads and other tablet devices, where

they believe there is a 'good reason' to do so. (This does not apply to indecent images – see below).

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 school rules

If indecent or obscene material, including pornography, is found/ suspected of being found on the device, the device must be passed to either the Headmaster, the Deputy Head or the DSL. Staff must not examine the device and they must ensure that the student has turned the device off.
Any searching of students 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 students' electronic devices will be dealt with through the school's complaints procedure.

7. Acceptable use of the internet in school
All members of the school community (staff, students, volunteers and governors) who have access to any aspect of the school's ICT network (login, email access, remote desktop, mobile devices)are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet.

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

We have software which monitors the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements.

8. Students using mobile and portable devices in school
Our policy is differentiated by year group as we believe that students should enjoying increased independence regarding their access to phones and mobile devices during the school day.
The key rule is that students must not access their phones while moving around the site and while they are in student accessed areas of the school site. Phones should also be switched off when students enter the school site. Other rules are differentiated according to year group.
Student accessed areas are as follows: Dining Hall, bottom court, middle court, top court, internal stair wells and stairs, corridors, toilets, public walkways around school, including the stairs from Lindsey House, New Hall, Olympic Torch Building to the top side of school and the Navigation Lane playing fields site, including the car park and pavilion and in transit to and from the site.

Whole School
Students are permitted to bring their phones into school. Students should switch off their phones when they enter the school site. Students are allowed to use their phone during the School day only under the direction of the class teacher during lessons or during an educational activity/ trip visit/ off-site activity with the approval of the trip leader. Students are aware that misuse of the privilege to use a phone for research/ learning/ music during a lesson can have implications on the rest of the class' opportunity to use their mobile device in that context. Posters are displayed around the school site explaining the rules and the sanctions.

The age groups are as follows:

1. Years 7-10
2. Year 11
3. Years 12 & 13

Years 7-10 are not allowed to have access to their mobile devices at all throughout the school day. It should be switched off as soon as they arrive on site. Access is permitted only in lessons where staff have given permission for their use. Students cannot have access to their phones at either morning or afternoon break or lunchtime in any public area or in classrooms. This includes the Library and O1.

Year 11 are not allowed to have access to their mobile devices at all throughout the school day EXCEPT in Elevenses, the Year 11 common room in the dining hall. Year 11 cannot use their phones in other areas of the dining room. Access is permitted only in lessons where staff have given permission for their use. Students cannot have access to their phones at either morning or afternoon break or lunchtime in any public area or in classrooms. This includes the Library and O1. Years 12 & 13 are not allowed to use their mobile device in public areas of the School or while moving around the site. They can have access to them in Casterby House, the Sixth Form area, the Library, O1 or in form and study rooms with the approval of a member of staff. Sixth Formers have more freedoms that other students in School but they also have greater responsibility to ensure that all members of the student community adhere to the policy. They can do this by avoiding the temptation to check phones while moving around the site.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

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 school. Any USB devices containing data relating to the school must be encrypted.

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

Work devices must be used solely for work activities.

The virtual desktop system is closely monitored and locked down so staff cannot install any software.

10. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in the 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 school'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. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school has a GDPR policy and procedures in place too.

The school 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 safeguarding training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings).

The DSL and deputies 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

Behaviour and safeguarding issues related to online safety are logged on SIMS/ in safeguarding folders.

This policy will be reviewed annually by the Headmaster. 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:

- GA Child protection and safeguarding policy
- CC Behaviour policy
- CD Anti-bullying policy
- DK Staff disciplinary procedures
- CH Data protection policy and privacy notices
- ED Complaints procedure
- GC Mobile phone and portable device policy
- GD Acceptable Use ICT policy