E-Safety Policy

February 2020

THE JO RICHARDSON
SUCCESS FOR ALL
COMMUNITY SCHOOL
ACHIEVE

Contents

Designated Safeguarding Lead: Callum Brierley

Head of Computing and ICT: Michael Campbell

ICT Network and Systems Manager: Daniel Trayler

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 (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school 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 students' 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.

3. Roles and responsibilities

3.1 The Governing Body

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

The Governing Body will co-ordinate meetings with appropriate staff to discuss online safety and monitor online safeguarding concerns as provided by the Designated Safeguarding Lead (DSL).

The Governor who oversees online safety is David Botteril.

All Governors will:

- Ensure that they have read and understood this policy;
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Acceptable Use Policy for Staff, Governors and Volunteers).

3.2 The Headteacher

The Headteacher 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 DSL and deputies are set out in our Safeguarding and Child Protection Policy as well relevant job descriptions.

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, ICT Network and Systems Manager and other staff, as necessary, to address any online safety issues or incidents;
- Ensuring that any online safeguarding incidents are logged on CPOMS and dealt with appropriately in line with this policy;
- Updating and delivering staff training on online safety;
- Liaising with other agencies and/or external services if necessary.

This list is not intended to be exhaustive.

3.4 The ICT Network and Systems Manager

The ICT Network and Systems 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 against viruses and malware, and that such safety mechanisms are updated regularly;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- 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.

3.5 All staff and volunteers

All staff, including contractors, 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;
- 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
- Hot topics - Childnet International
- Parent factsheet - Childnet International
- Reporting online abuse to the police - CEOP
- Online safety support - NSPCC Online Safety

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. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Educating students about online safety

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

During **Key Stage 3**, all 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;
- 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 secondary school**, 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 (eg, 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 jail;
- 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.

The school will use 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 via The Seagull, and in information through our school website. This policy will also be shared with parents through the website.

Online safety information may also be shared during Progress Evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with their tutor who will in turn pass on if required to Head of Year, DSL and Headteacher.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

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 Tutors may 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 in PDE, Computing/IT, form time and other subjects where appropriate.

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

The school also sends information 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. This is signposted on our school website.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy and anti-bullying 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 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

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.

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 inappropriate material is found on the device, a member of the Safeguarding Team or 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 school discipline); and/or
- Report it to the police.

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 students, staff, volunteers and Governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

8. Students using mobile devices in school

JRCS is a 'mobile free zone'. Students must not use or show their mobile phones at any point whilst they are in the school building or grounds. They may have their phones switched off in their bags and lockers.

If such items are brought into school, students do this at their own risk.

In the event of an emergency where parents need to contact a student, they must telephone the school reception. Students are never to use their mobile phones to communicate with parents during the school day. Such use will result in sanctions for the student and confiscation of the phone.

If students do use a mobile phone during the school day it will be treated as a banned item.

9. Acceptable use by staff

Please refer to our Acceptable Use Policy. This is a document signed by staff when commencing their employment at the school.

10. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, the action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. A decision will be made on whether the misuse is accidental and non-malicious or if it is intentional and malicious. The behaviour will be levelled in accordance with our behaviour policy and sanctioned appropriately. This may include a period of time in which a student will have their ICT access limited.

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 school's disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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 through their Hays Online Safeguarding Training. Staff will also carry out online GDPR training.

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 and staff meetings).

The DSL and Deputies will undertake child protection and safeguarding training, which will include online safety, at least every two 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 Safeguarding and Child Protection Policy.

12. Monitoring arrangements

The DSL and Deputies will log safeguarding issues related to online safety through the school's Child Protections Online Monitoring System (CPOMS). Behaviour incidents related to online safety will be recorded on as a Cause For Concern (CFC) - see behaviour policy.

This policy will be reviewed every two years by the DSL. At every review, the policy will be shared with the Governing Body.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding and Child Protection Policy
- Behaviour Management Policy
- Anti-Bullying Policy
- Whistleblowing Policy
- Data Protection Policy
- Code of Conduct
- Complaints Policy
- Acceptable Use Policies