Online Safety Policy

THE SPIRES
COLLEGE

Adopted:	November 2019	Review Due:	October 2021
Reviewed:	July 2020	Revised:	July 2020 Mobile Phone rule updated

Aims

The College 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 college community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

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 Board

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

The governing board will include online safety in its safeguarding monitoring activity.

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.

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 (DSL)

Details of the college's DSL and deputies are set out in our Child Protection and Safeguarding Policy as well as in 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 recorded and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with our Behaviour Policy and Anti-Bullying Policy;
- Updating and delivering staff training on online safety;
- 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 students 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 regularly, as appropriate;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- Ensuring 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's Behaviour Policy and Anti-Bullying 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, and ensuring that students follow the college's terms on acceptable use;
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with our 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 that they have and their child has read, understood and agreed to the terms on acceptable use of the college's ICT systems and internet (ICT Acceptable Use Policy and Agreement).

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 expected to agree to the terms of our ICT Acceptable Use Policy and Agreement.

4. Educating students about online safety

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

From September 2020 **all** schools will have to teach Relationships and sex education and health education in secondary schools.

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

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 (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 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 college will use assemblies and may also invite speakers to raise students' awareness of the dangers that can be encountered online.

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 social media accounts. This policy will also be shared with parents.

Online safety will also be covered at information sessions during parents' evenings. Further literature for parents is available in College Reception. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL.

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

We will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Staff will discuss cyber-bullying within tutor groups and in relevant lessons, and the issue will be addressed in assemblies. Teaching staff are 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 receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

The college also provides 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.

In relation to a specific incident of cyber-bullying, the college will follow standard college sanctions as set out in the college Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among students, the college will use all reasonable endeavours to ensure the incident is contained. The incident will be reported to the police if it involves illegal material, and the college 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 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 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 our complaints procedure.

7. Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the college ICT systems and the internet. 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 students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in our Acceptable Use Policy and Agreement document.

8. Students using mobile devices in school

Although the college prefers that they do not, students are permitted to bring mobile telephones on to the college site. However, these must not be used, seen or heard on site at any time. Students must ensure that mobile phones are switched off and placed securely in their school bag before they enter the college gates. The sanction for breaching this rule is confiscation.

The college is not responsible for personal belongings that are brought into college.

The college follows Government advice when confiscating items from students which is outlined in the document 'Screening, Searching and Confiscation - Advice for Schools,' January 2018.

The college will confiscate any electronic items being used inappropriately on the premises such as mobile phones.

- ▲ On the first occasion the item will be confiscated until the end of the **next** college day;
- ▲ On a second occasion the item will be confiscated for one week;
- ▲ On a third occasion the item will be confiscated until the end of term.

Any further issues with a phone or electronic device will result in a meeting with the Principal. Should the situation reach this stage, a permanent ban on bringing the item into college is likely.

If a student refuses to surrender the item, a member of the Senior Leadership Team (SLT) will become involved and, if the situation reaches this point, the confiscation will be increased by the member of the SLT to one week, or longer if appropriate. Further sanctions will also be imposed.

The SIM card and battery will be confiscated along with any mobile phone.

Students who have had their mobile phone confiscated and need to contact their parents/carers must speak to their Head of Year or Pastoral Support Manager.

9. Staff using work devices outside school

Staff members using a college device outside of school 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 our Acceptable Use Policy and Agreement.

Staff must ensure that their college 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.

College devices must be used solely for work activities.

10. How the college will respond to issues of misuse

Where a student misuses the college's ICT systems or internet, we will follow the procedures set out in our Behaviour Policy and ICT Acceptable Policy and Agreement. 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 and/or staff Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The college will report incidents that involve illegal activity or content to the police and consider if other 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 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

The DSL or appropriate pastoral leader logs behaviour and safeguarding issues related to online safety on SIMS or CPOMS, as appropriate.

This policy will be reviewed every three years.

13. Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Disciplinary Procedures
- Staff Code of Conduct
- Data Protection Policy and Privacy Notices
- Complaints Procedure
- ICT Acceptable Use Policies and Agreements