Online safety policy

Arun Court School

Contextual Statement
As a school that has been recognized by Surrey LEA as 'providing for some of the county's most vulnerable children many of whom have been difficult to place' and recognized by Ofsted as 'unique' we are very aware of the importance of our context.
Teenagers find it difficult to assess risk, and our teenagers have added complexities and vulnerabilities that will further hamper their decision making. Some students spend a great deal of their free time on technology and a few are at the point where they are clinically addicted to technology use. Technology is a place where our young people feel braver and safer, compared to real world interactions – and that extra confidence poses additional risks as they are likely to be more trusting online.

Approved by:	James White	**Date:**	3/2/2021
Last reviewed on:	3/2/2021		
Next review due by:	3/2/2023		

Contents

---

1. Aims

Our school 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 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 DfE'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.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the 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 EMAT member who oversees online safety is Paul Phillips.

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 (appendix 2)

3.2 The Principle Of School

The principle of school 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 child protection and safeguarding policy as well as 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 principle of school and associated principle, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately 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
- Providing regular reports on online safety in school to the headteacher 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 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
- 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

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 (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendices 2)
- 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 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 principle of school 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 (appendices 1)

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
- Healthy relationships – Disrespect Nobody

3.7 Visitors

Visitors 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 (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the 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

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 secondary school**, pupils 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.

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. This policy will also be shared with parents.

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

Concerns or queries about this policy can be raised with any member of staff, principle of school or associate principle.

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 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 school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their groups.

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, and EMAT members have received training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

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 pupils, 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 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 school 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 pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and the school's COVID-19 risk assessment.

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

7. Acceptable use of the internet in school

All pupils, parents, staff and EMAT members 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 pupils, staff and EMAT members (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement

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

Mobile devices are handed in first thing in the morning and handed back during breaktimes only. Staff will monitor what the students are watching and searching for, this will be reported to the principle of school if any suspect material has been witnessed. If deemed safe the mobile device will be returned at the end of the school day.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Work devices must be used solely for work activities.

Staff sign a technology agreement stating that all rules will be adhered to.

If staff have any concerns over the security of their device, they must seek advice from Stuart Mason the ICT manager at itsupport@bravura.info

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and internet acceptable use. 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 code of conduct. 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.

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.

The DSL and deputy 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. We get regular updates from CASPER and will cover any relevant aspects at staff meetings.

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

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

12. Monitoring arrangements

This policy will be reviewed every 2 years by the Senior Leadership Team. At every review, the policy will be shared with the EMAT members..

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff code of conduct
- Data protection policy and privacy notices
- Complaints procedure

- ICT and internet acceptable use policy

Appendix 1

ICT & Personal technology permissions form and agreement

This form to be returned BEFORE you can bring in personal devices please

Personal Tech:

We assume absolutely no liability for any technological or personal device that is brought on to the premises. Users do so entirely at their own risk and this includes intentional or accidental damage by students or staff

Students aged under 15 will hand in their phone to the safe if it is on the premises – if they need to call home we will provide a facility for them to do so

All students will be asked to hand in their phone at the start of each lesson, or to place it away for the duration of the 45 minute lesson. If bullying occurs via phone use during breaks the perpetrator will not be allowed to bring in their phone, ever. If students access pornography, racist, homophobic, or other unsuitable material during breaks the perpetrator will not be allowed to bring in their phone, ever. If the student requires music to help them study then they may use an MP3 player.

At all times they will play games in full view of a member of staff and staff will remove the device if an unsuitable game is being played. Students are not allowed to access you-tube on their devices. Students accessing unsuitable material (see the above point) will not be allowed to bring in their devices, ever. At the end of breaks students are expected to hand their devices back in, continual refusal to do so or rudeness to staff, will mean that they will not be able to bring their devices in or borrow centre ones for leisure purposes

Students who do not have their own tech to bring in may play games on a centre ipad, or lap top, subject to availability. We ask that games are not downloaded as this clogs up the memory space – if you wish to request a game to be downloaded you may do so

Centre tech:

We have blocking systems in place but these are not failsafe, none are. Students MUST report any unsuitable material that pops up or is accessed accidentally.

Students must treat devices with respect – breakages will be charged

Students using the internet or email need to remember the centre guidance around their own safety and around ensuring that they do not have cause to regret posts or emails that they send. Students should NEVER place their personal details into search engines or in communication with others online

Centre tech should only be used when there is an adult in the room able to observe and supervise

DATA protection

Students may not photograph or record lessons, staff or other students on their own devices. They should not do so on centre devices unless it is part of a planned activity, with adult supervision.

We keep student passwords for Futurelearn, IXL and other online packages confidential – we expect students to do the same

I understand and agree to support the centre in this agreement

Parent signature …… Date ……

I agree to abide by this agreement

Student signature …… Date ……..

Appendix 2: acceptable use agreement

Arun Court Technology Agreement

In accepting the use of a Arun Court School ICT, I agree to the following conditions:

1. I understand that I am solely responsible for the use of any ICT equipment while in use.
2. I shall only use the ICT equipment in relation to work related purposes.
3. I shall treat all ICT equipment as if it was my own and will notify I.T. Services of any defect or malfunction during my use.
4. I shall not install and / or download any unauthorised software and / or applications
5. I shall not allow the ICT equipment to be used by an unknown or unauthorised person.
6. I assume the responsibility for the actions of others while using the ICT.
7. Any work saved on the ICT will be deleted by IT services on the next computer maintenance.
8. If the ICT is damaged, the incident must be reported to Stuart Mason who can be emailed on itsupport@bravura.info or James White on enquiriesbigbeareducation@outlook.com within 24 hours.
9. If the lost, stolen or damaged ICT and / or accessories is determined to be caused by negligence or intentional misuse, I shall assume the full financial responsibility for repair costs or fair market value of the ICT.
10. I am aware that any breach of these policies may render me liable to disciplinary action under the company's procedures.

Signed:

Name:

Date: