Biddenham International School & Sports College

E-SAFETY/ONLINE SAFETY POLICY

Aims

Our school aims to:

- Have robust processes in place to ensure the E-Safety\Online safety of students, staff, volunteers and governors.
- Deliver an effective approach to E-Safety\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.

Legislation and Guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying. It also refers to the Department's guidance on protecting children from radicalisation. It also takes into account the Peer on Peer processes in school.

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 also takes into account the National Curriculum Computing Programmes of Study.

Roles and Responsibilities

- Governing Body:

  Has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

  Will co-ordinate regular meetings with appropriate staff to discuss E-Safety\Online safety, and monitor E-Safety\Online safety logs as provided by the designated safeguarding lead (DSL).

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.

- Principal:

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

- Designated Safeguarding Lead:

  Details of the school's designated safeguarding lead (DSL) and team are set out in our Safeguarding and Child Protection policy.

The DSL, supported by the Safeguarding team, coordinates the E-Safety\Online safety in school, in particular:

  Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.

  Working with the Principal, ICT manager and other staff, as necessary, to address any E-Safety\Online safety issues or incidents.

Ensuring that any E-Safety\Online safety incidents are logged 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 the school behaviour management policy.

Updating and delivering staff training on E-Safety\Online safety.

Liaising with other agencies and/or external services if necessary.

Providing regular reports on E-Safety\Online safety in school to the Principal and/or governing board.

This list is not exhaustive.

- ICT Manager

The ICT Manager is responsible for:

Putting in place appropriate filtering and monitoring systems, which are maintained 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 "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.

Conducting security checks and monitoring the school's ICT systems throughout the week.

Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

Ensuring that any E-Safety\Online safety incidents are reported to the safeguarding team so they can be appropriately dealt with in line with this policy.

Ensuring that any incidents of cyber-bullying are reported to the safeguarding team and support is provided so that the incident can dealt with appropriately and in line with the school Behaviour Management policy.

Ensuring that another member of the IT Support team is able to provide support in the event of the ICT Manager's absence.

This list is not exhaustive.

- 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.

Working with the DSL to ensure that any E-Safety\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 behaviour management policy.

This list is not exhaustive.

- Parents\Carers

Parents\carers 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 school's ICT systems and internet.

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

What are the issues?, UK Safer Internet Centre:

www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues

Hot topics, Childnet International: www.childnet.com/parents-and-carers/hot-topics

- 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.

Educating students about E-Safety\Online Safety

Students will be taught about E-Safety\Online safety as part of the KS3 curriculum, during transition and through our Essential Life Skills delivery and taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- Recognise inappropriate content, contact and conduct, and know how to report concerns.

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.

Educating parents\carers about E-Safety\Online safety

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

If parents\carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the head of year and escalated as required to the DSL or Principal.

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

Cyber-bullying

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's Behaviour Management policy.)

- 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 in ELS\tutor time, and the issue will be addressed in assemblies at the start of the year. Follow up sessions will run throughout the year to tackle individual and school-wide issues as they are identified.

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 'Training' section below for more detail).

The school also sends online safety information/leaflets to parents/carers via the school website so that they are aware of the signs, how to report it and how they can support children who may be affected. Parents/carers are invited to take part in online courses through our links to Online Safety Alliance.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour Management 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.

- 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, it is up to the staff member in conjunction with the DSL or other members 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 regarding searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school Complaints Procedure. The DSL in conjunction with the relevant member of staff will decide on the next course of action namely MASH Referral (Multi-Agency Support Hub) or involvement of the Police as necessary.

Acceptable use of the internet in school

All students, parents\carers, 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 primarily be for educational purposes, or for the purpose of fulfilling the duties of an individual's role. Sensible recreational use of the school's internet connection can take place at break and lunch times provided it does not impede the functionality of the network (excessive bandwidth usage), infringe on copyright, and bring professional self or the school's reputation in to disrepute.

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

Students using mobile devices in school

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

- Lessons
- Tutor group time.
- Clubs before or after school, or any other activities organised by the school.

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

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school's Behaviour Management policy, which may result in the confiscation of their device.

Staff may allow an exception to the rules in the event of a Safeguarding event/issue.

Staff using work devices outside school (GDPR)

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, as set out in the school's ICT Acceptable Use policy.

Unauthorised software is defined as:

- Software, apps, websites or browser extensions which could bypass/circumvent the schools security/web filtering.
- Share data by using a non-Google service (such as other cloud storage services) as set out in the school's Staff Cloud Services policy.

If staff are unsure, would like clarification or would like to use some new software please contact the IT Support Helpdesk.

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.

Staff should not allow anyone else to use their chromebook while logged into their account (this would put school data at risk).

Staff may use USB devices containing data relating to school work as long as it contains no sensitive data (student data, etc) and as best practice the device should also be encrypted.

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

Work devices must be used primarily for work activities but we do not mind staff doing research, shopping etc as long as the account is secure.

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

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 safeguarding team 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 online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to this policy.

This policy will be reviewed yearly by the IT Network Manager. At every review, the policy will be shared with the governing board.

Links to our school policies:

- Safeguarding and Child Protection
- Behaviour Management
- Code of Conduct
- Complaints Procedure
- Bring Your Own Device (BYOD)
- ICT Acceptable Use

Date of Next Review: **June 2022**