Kingsbrook School

E-Safety and IT Use Local Procedure

Kingsbrook School
Southburgh
Thetford
Norfolk IP25 7TJ

6th January 2025
Review: 6th January 2026

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

Legislation and guidance

This procedure is based on the Department for Education's statutory safeguarding guidance, Keeping Students Safe in Education, 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 students 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 Head of School

The head of school is responsible for ensuring that staff understand this procedure, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) are set out in our local procedure.

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

Ensuring that staff understand this procedure and that it is being implemented consistently throughout the school

Ensuring that any online safety incidents are logged and dealt with appropriately in line with this procedure

Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour procedure

Liaising with other agencies and/or external services if necessary

All staff

All staff, including contractors and agency staff, and volunteers are responsible for:

Maintaining an understanding of this procedure

Implementing this procedure consistently

Agreeing and adhering to the terms on acceptable use of the IT on site

Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this procedure

Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour procedure

This list is not intended to be exhaustive.

Parents / Carers

Parents are expected to:

- Notify a member of staff or the head of school of any concerns or queries regarding this procedure
- 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 students 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

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 procedure, when relevant, and expected to read and follow it.

Educating students about online safety

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

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 and 5** 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 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 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 procedure will also be shared with parents / carers.

Online safety will also be covered during open days.

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 school and/or the DSL.

Concerns or queries about this procedure can be raised with any member of staff or the head of school.

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 procedure.)

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.

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.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour procedure. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavors 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.

Students using mobile devices in school

Students may bring mobile devices into school but are not permitted to use them. The mobile telephone procedure is to be followed.

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 procedure. 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.

Student Email Accounts

Students are provided with email accounts and addresses when they join Kingsbrook School. These accounts are monitored, and students are provided with the following information:

Monitoring

You should be aware that emails sent or received via Aspris email may be stopped and checked by IT for a variety of purposes, including, but not limited to, ensuring compliance with our internal policies and supporting internal investigations.

Emails and Cyber Security

The internet can be an unsafe place, so you should take care when using email against the cyber risks

You must be extremely careful when opening email attachments that are from senders that you do not know, as it may contain a computer virus that could harm your equipment.

You should be aware that senders you do not know may be trying to trick you so that they can steal your personal information, such as usernames, passwords and confidential information. Some emails may ask you to reply or complete and return an attachment. If this happens you must not do this and inform your teacher/tutor straight away.

Under no circumstances are you allowed to use your email in any illegal activity. The following activities are **strictly forbidden**, with no exceptions when using Aspris email:

1. Aspris email must not be used to send or forward emails or documents containing harassing or offensive messages, including offensive comments against protected characteristics- race, gender, hair colour, disabilities, age, sexual orientation, religious beliefs and practice, political beliefs, or national origin. If you receive any emails with this content from anyone, you should report the matter to your teacher/tutor straight away.
2. You must not use your Aspris email to set up social media accounts, or purchase items online.
3. You must not use another person's email account to send unwanted email messages or attempt to forge email messages or send email.
4. You must not send chain letters or joke emails from your email account.
5. You must not breach copyright or licensing laws when creating and sending emails or include attachments that contain software, music, digital photos, books or logos not belonging to you.
6. You must not make false offers of products or services from your email account.
7. You must not complete any form of monitoring which will stop emails intended for other email accounts.
8. You must not send any kind of message to any other user in or outside of Aspris email system (for example, denial of service attack).
9. You must not send information about your school/college staff or other Aspris staff or students to people in or outside of Aspris.
10. You must not send unwanted email messages, including the sending of "junk mail" or other advertising material to individuals who did not request such material (email spam),
11. You must not undertake or take part with others in any form of harassment via email as this is seen as Cyberbullying.

If you do not follow these rules, Aspris reserve the right to remove your email account.