Online Safety Policy

Version Control

Contents

1. **Rationale**

1.1 New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. These technologies can stimulate discussion, promote creativity and enhance effective learning. Children and young people should have an entitlement to safe internet access at all times and the Kingsbury Green Academy Online-Safety policy will help to promote and ensure safe and appropriate use of the internet and related technologies, by involving all stakeholders in our children's education. The internet and other digital technologies can put young people at risk within and outside the school and it is the duty of care of all who work within the school as well as parents and the wider school community to protect our children from these dangers. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to/loss of/sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this online-safety policy is used in conjunction with our other policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

2. **School responsibilities:**
Introduce ICT to pupils

2.1 A module on responsible internet use and digital safety will be included in the curriculum covering both school and home use. This will include the necessity of keeping personal information safe, how to use mobile technologies appropriately and using online communication appropriately. Instruction on responsible and safe use should precede internet access.

2.2 The topic of digital safety, including cyber bullying, will also be addressed through key stage 3 ICT lessons and supported in Year 7-9 PSE lessons.

Use the internet to enhance learning

2.3 Pupils will learn appropriate internet use and be given clear objectives for internet use. Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.

2.4 Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Help pupils learn to evaluate internet content

2.5 Specific lessons will be included within the IT Scheme of Learning that teaches all pupils how to read for information from web resources. Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

Authorised internet access

2.6 All pupils must agree to the Acceptable Use Policy each time they log on to the school network, a copy of which is sent to parents annually.

Enforce online communications, social networking and mobile technology school rules

2.7 The use of online chat via social media sites is not permitted in school. Other social networking sites are routinely blocked through the school's filtering service.

2.8 Pupils are permitted to bring mobile phones to school, but they must be switched off during lessons and are only allowed to be turned on at the end of the day.

2.9 Pupils may not use mobile phones to film other members of the Kingsbury Green Academy community without their permission.

2.10 The consequences of inappropriate use of the internet, or mobile phones, will be clear to pupils as is outlined in the Behaviour for Learning (B4L policy).

Manage filtering

2.11 Agile ICT have implemented a web filtering service which is hosted by the FortiGate firewall. This service filters internet access by cross-referencing all website requests against the Fortinet online threat service, named FortiGuard. FortiGuard is continually updated by the Fortinet global security research team, who assign websites to categories based on the content they deliver. In addition to the Fortiguard based category filtering, Kingsbury Green Academy can explicitly permit or deny individual sites that they feel appropriate for any duration required via request to the Agile Helpdesk. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to Agile via the Office Manager who will inform the IT Technicians.

Agile is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack;
- that the school meets e-safety technical requirements
- is using effective filtering and monitoring service in accordance with the Prevent agenda;
- that users may only access the school's networks through a properly enforced password protection policy.
- that students have limited access to the internet via 3G and 4G on the school premises
- 'overblocking' does not lead to unreasonable restrictions as to what the students are taught with regards to online teaching and safeguarding.

* Keeping children safe in education 2016 (p62/63)

Assess Risks

2.12 The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Kingsbury Green Academy cannot, therefore, accept liability for the material accessed, or any consequences of internet access.

Manage Website Content

2.13 The Assistant Headteacher with responsibility for Safeguarding will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.14 Parents will be given the opportunity to say if they are not happy for their child's photograph to be published.

Manage pupil e-mail

2.15 All pupils will be issued with a school e-mail account. E-mail is intended to allow collaboration with staff and other pupils in subject related activities. School e-mail is not for personal/social use. Pupils will be clear that e-mail communication is not confidential. E-mail can be accessed at home or in school and parents are encouraged to look at their child's school e-mail account. All pupils will be taught how to use the e-mail system and the rules that apply to it. All pupils have to agree to the school Acceptable Use Policy each time they log on to the network. Any pupil found to be in breach of this policy may have their access withdrawn.

E-mail rules

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.
- Pupils should use e-mail in an acceptable way. Sending images without consent, messages that cause distress and harassment to others are considered significant breaches of school conduct and will be dealt with accordingly.

In addition:

- Access in school to external personal e-mail accounts may be blocked.
- Access to e-mail will be restricted to specific times during the school day.

Inform parents

2.16 Parents' attention will be drawn to the School Online Safety Policy through the school website.

Manage staff e-mail

2.17 Staff e-mail addresses will not be published. All subject related e-mail correspondence from parents will be forwarded to the relevant department or staff member. This email address admin@kingsburygreenacademy.com.

Inform staff and governors of their roles and responsibilities with regard to online safety

2.18 All governors and staff, including teachers, supply staff, teaching assistants, cover supervisors and support staff, will be provided with the school Online Safety Policy and its importance explained.

2.19 The school's consequences for internet and mobile phone misuse will be clear so that all teachers are confident to apply this should the situation arise.

2.20 All staff must accept the terms of the 'Responsible Internet Use' statement before using any internet resource in school.

2.21 Staff should be aware that internet traffic is monitored and reported by Agile and can be traced to the individual user. Discretion and professional conduct is essential.

Follow school procedure for dealing with any complaint about staff misuse

2.22 Any complaint about staff misuse must be referred to The Principal. See Staff Code of Conduct.

The nominated person for the implementation of the online safety policy is the Head of Enterprise and Creative Technology department.

3. Use of digital and video images

3.1 When using digital images, staff will inform and educate pupils/students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they will recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.

- Staff are allowed to take digital/video images to support educational aims, but will follow school policies concerning the sharing, distribution and publication of those images. School equipment can be provided for taking photos, videos or sound recordings linked to an educational intention, but it is appreciated that own devices may be easier.
- Photographs/videos published on the website, or elsewhere that include pupils/students will be selected carefully and will comply with good practice guidance on the use of such images.
- With regard to parental permission, the school follows an 'opt out' scheme rather than obtaining permission from parents.

4. Unsuitable/inappropriate activities

4.1 The School believes that the activities referred to in the following section are inappropriate in a school context and that users, as defined below, will not engage in these activities in school or outside school when using school equipment or systems.

Users will under no circumstances:

- Visit internet sites, make, post, download, upload or pass on material, remarks, proposals or comments that contain or relate to:
- pornography (including child pornography)
- promoting discrimination of any kind or promoting racial or religious hatred
- promoting illegal acts

- Use the internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could be considered inappropriate.

In addition, staff will not:

- engage in any contact with a pupil via social networking sites which are not approved for use by the School Senior Leadership team, share personal contact information (mobile phone numbers, home email address, etc.) with pupils. Should staff require the personal mobile phone numbers of pupils in order to contact them on an educational trip/visit, the school mobile telephones will be used wherever possible. In any event, the contact details of pupils will then be erased from the mobile device as soon as the trip/visit has returned safely.

4.2 **Responding to incidents of misuse**

The E Safety Coordinator and Designated Safeguarding Lead will be informed immediately of any apparent or actual misuse which appears to involve illegal activity, i.e.:

- child sexual abuse images;
- adult material which potentially breaches the Obscene Publications Act;
- criminally racist material;
- other criminal conduct, activity or materials.

The E-Safety Coordinator or Designated Safeguarding Lead will then instigate the School Protocol on Child Protection and E-Safety.

5. Data Protection

5.1 Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018 (GDPR) which states that personal data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- kept no longer than is necessary;
- processed in accordance with the data subject's rights;
- secure;
- only transferred to others with adequate protection.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data;
- do not allow students to log on as staff.

6. Parents and carers responsibilities.

6.1 It is hoped that parents and carers will support the school's stance on promoting good internet behaviour and responsible use of IT equipment both at school and at home. The school expects parents and carers to sign the school's acceptable use polices, indicating agreement regarding their child's use and also their own use with regard to parental access to school systems such as websites, forums, social media and questionnaires. The school will provide opportunities to educate parents with regard to e-safety, including:

- Evening sessions or a series of presentations run by the school for parents and wider school community stakeholders.
- Online-safety information delivered to parents directly, including: SchoolComms and through the website.