Kingsweston School

E-Safety Policy

Kingsweston School

E-Safety Policy

Introduction

At Kingsweston School we take Internet Safety very seriously and see it as our duty to keep our pupils safe whilst using technology, acquiring skills and understanding in school and applying these not only in school but also at home. This also includes our responsibility to keep our children safe from radicalisation and extremism (Prevent Duty).

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at regularly and in response to any e-safety incident to ensure that the policy is up to date and ensure effective in supporting the effective management of any incidents.
- Appoint a governor to have overall responsibility for the governance of e-safety at the school who will:
    - Receive regular updates from the school in regards to training, identified risks and any incidents.
    - Chair the e-Safety Committee

E-Safety Committee

The E-Safety Committee includes at least one nominated governor, staff representatives (including representatives from both strands and a minimum of one senior leader), the school network/IT manager, a parent (could be a parent governor), the Pastoral and Safeguarding Mentor.

The E-safety Committee is responsible for:

- Advising on changes to the e-safety policy.
- Establishing the effectiveness (or not) of e-safety training and awareness in the school.
- Recommending further initiatives for e-safety training and awareness at the school.

Network Safety

The school's Network is looked after by our network/IT manager.

Frequent meetings between the network manager and the Business Manager take place. During these any issues with the Network and E-Safety issues are identified, dealt with and/or raised as an issue to be dealt with more widely, as necessary.

Bloxx web filtering is used in school as part of the school's support for keeping pupils safe online. Sophos antivirus protects our infrastructure along with automatic Windows updates generated through the use of WSUS.

Security is further enhanced as all computers at the school run user security policies which prohibit pupils from running or installing any programs or applications. This is designed to stop any unwanted programs such as malware or inappropriate applications from being used or installed on the network/computers.

The network/IT manager will ensure that:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
- Any e-safety technical solutions such as Internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age/needs of the user.

All staff, pupils (as far is relevant and meaningful) and parents/carers will be informed that Internet activity may be monitored in order to ensure as much as possible that users are not exposed to illegal or inappropriate websites, and to ensure as much as possible that users do not actively seek access to illegal or inappropriate websites

Safety and Responsibilities for Staff

This section should be read in conjunction with the Acceptable use of ICT Facilities policy and our Code of Conduct.

The Code of Conduct and Acceptable use of ICT Facilities documents reference the responsibilities of all staff and covers the use of digital technologies in school and they complement the General Teaching Council's Code of Practice for Registered Teachers. They should be read alongside the following expectations:

1. I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
2. I will not reveal my password(s) to anyone. I will not log on for another person.
3. I will not allow unauthorised individuals to access E-Mail/Internet/Intranet/network, or other school/LA systems and understand that doing so may break data protection and confidentiality laws.
4. I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
5. I understand that there is a difference between my professional and private roles. I will not engage in any online activity that may compromise my professional responsibilities, this refers to social network sites such as Facebook.
6. I will only use the approved, secure E-Mail system(s) for any school business.
7. I will only use the approved school E-Mail or other school approved communication systems with pupils or parents/carers, and only communicate with them in relation to appropriate school business.
8. I will maintain appropriate relationships and boundaries with pupil and parents/carers when using school E-Mail or other school approved communication systems.
9. I will not at any time use school equipment to browse, download or send material that could be considered offensive or inappropriate to colleagues or pupils.
10. I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to my line manager.
11. I will not download any software or resources from the Internet that can compromise the network, or that are not adequately licensed.
12. I will not connect a computer, laptop or other device (including USB flash drives), to the network/Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other IT 'defence' systems by bringing the equipment into school and connecting to the school network at least once a month to receive all necessary updates.
13. I will not use personally owned digital cameras or camera phones for taking and transferring images of pupils or staff and will not store images at home.
14. I will ensure that any private social networking sites/blogs etc. that I create or actively contribute to cannot be confused with my professional role.
15. I agree and accept that any computer, laptop or IPad loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school if a reasonable amount of personal use outside of school hours becomes "significant personal use" as defined by HM Revenue & Customs.
16. I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
17. I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
18. I will embed the school's E-Safety principles into my teaching.

19. I will only use LA systems in accordance with any corporate policies.
20. I understand that all Internet usage/and network usage is monitored and that monitoring data could be made available to my manager on request.
21. I understand that failure to comply with this agreement could lead to disciplinary action.

Safety and responsibility for Pupils

Although some of our pupils are unable to access the Internet we have a good percentage of pupils who are able to use it independently and therefore are at risk from either deliberately accessing inappropriate material or, due to their level of literacy, accidently accessing harmful sites. These include risks associated with Child Sexual Exploitation, radicalisation and extremism and this policy should be considered within the context of the school ethos and other relevant policies (e.g. Spiritual Moral Social and Cultural provision) for the purpose of protecting pupils from such dangers.

No pupil is able to access the Internet in school without their parents giving permission for them to do so. This consent form is filled in when the pupil starts school and is kept on record until they leave; it will only need amending if a parent/carer would like to change it.

All pupils who are able will have to sign an agreement and this will be completed every year within the context of an E- Safety session. This document clearly states their responsibilities when using technology in school. Staff will monitor internet access at all times in school to ensure that the sites visited are consistent with the vision and values of the school and our duty to protect pupils and promote British values.

All pupils will be taught how to use all technologies in a responsible and safe way. This is a specific part of the IT curriculum and reference to E-Safety is embedded throughout the curriculum offer.
No pupil may appear on the Web Site without their parent/carers consent, the consent form is completed when the pupil starts school and is kept on record until they leave; it will only need amending if the parent/carer would like to change it.

Support for Parents

As a school we believe it is our duty to support parent and carers in keeping their child safe while using technology. Computers and other devices in the home are more open and don't have the security features which we have in school, which does make the child more vulnerable in this environment.

The school web site will have information regarding E-Safety for parents/carers and young people.

Appendix 1

Why do we Filter and Monitor?

Filtering:	This is a pro-active measure to ensure (as much as possible) or prevent users from accessing illegal or inappropriate websites.
Monitoring:	This is a reactive measure and for the most part means searching, browsing or interrogating filter logs (known as the cache) for Internet misuse.

We filter to ensure:

- (As much as possible) that children and young people (and to some extent adults) are not exposed to illegal or inappropriate websites. These sites are (or should be) restricted by category dependent on the age of the user. Exposure would include browsing to specifically look for such material, or as a consequence of a search that returns inappropriate results.
- (As much as possible) that the school has mitigated any risk to the children and young people, and thereby reduces any liability to the school by making reasonable endeavours to ensure the safety of those children and young people.

We monitor for assurance:

- (As much as possible) that no inappropriate or illegal activity has taken place.
- To add to any evidential trail for disciplinary action if necessary.

A right to privacy?

Everybody has a right to privacy, whether adult or child. But in certain circumstances there is a reduced expectation of privacy. In the context of this policy, that reduction is for security and safeguarding. This expectation is applicable whether it is school-owned equipment, or personally owned equipment used on the school network (and in some cases even if that personally owned equipment isn't used on the school network, but is used in school or for school business).

Managing Expectations

It is the expectations of the user that is particularly important; this will include school staff, students and parents/ carers of the pupils. Consent is not a requirement.

Ofsted make clear that schools should be managing their own filter, and this would include monitoring for inappropriate activity.

Explaining to parents, staff and students

It is the understanding that is important, (as far as is practicable within the context of a learning difficult orientated school) not the consent. This will be shared through the website, through this policy, through IT and PSHE teaching within school and through the Code of Conduct and Acceptable Use policies.