E-Safety Policy

SCOPE:	Academy Policy
AUTHOR/ORIGINATOR:	E-Safety Champion / Principal
NAME OF RESPONSIBLE DIRECTOR/PRINCIPAL:	Sector Director
APPROVING COMMITTEE:	Sector Director
STATUTORY BASIS:	Non-Statutory Policy
REQUIREMENT TO PUBLISH ON WEBSITE:	No
DATE RATIFIED:	July 2024
DATE DISTRIBUTED TO STAFF:	July 2024

Table of Contents

1. Introduction 3
2. Development / Monitoring / Review of this Policy 3
3. Schedule for Development / Monitoring / Review 3
4. Scope of the Policy 4
5. Roles and Responsibilities 4
7. Employees 4
10. Teaching and Learning 6
11. Benefits of using the Internet in Education 6
13. Managing Internet Access 6
14. Use of Email 7
15. Published Content – Website 7
16. Social networking and personal publishing 7
17. Emerging technologies 8
18. Personal data 8
19. Internet Access 8
20. Risk Assessment 8
21. E-safety complaints 8
22. Internet used across the community 9
23. Communications Policy 9
24. Parental Support 9

1. Introduction

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Schools must, through their e-safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. The policy will also form part of the school's protection from legal challenge, relating to the use of digital technologies.

2. Development / Monitoring / Review of this Policy

This e-safety policy has been developed by Achievement Lead for Computing. The E-safety committee made up of:

Designated Safeguarding Lead: **Mrs M Lawson**

Other staff trained to deal with safeguarding concerns:

- **Mrs L Pollock –** Deputy Designated Safeguarding Lead

Safeguarding Governor: **Mrs M Marsh**

Deputy Safeguarding Lead and Anti-Bullying Champion: **Mrs A Simpson**

E-Safety Champion: **Mr J Dighton**

Consultation with the whole school community will take place through a range of formal and informal meetings.

3. Schedule for Development / Monitoring / Review

- This e-safety policy was approved by the Academy Advisory Committee.
- The implementation of this e-safety policy will be monitored by the Principal.
- Monitoring will take place at regular intervals: **at least once a year**
- The Academy Advisory Committee will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals: **at least once a year**

- The E-Safety Policy will be reviewed every 3 years, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be: **July 2027**

- Should serious e-safety incidents take place, the following external persons / agencies should be informed: **Trust ICT Manager, Trust Safeguarding Officer, Police**

The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Monitoring logs of internet activity (including sites visited) – providing adequate software is purchased.
- Internal monitoring data for network activity – providing adequate software is purchased.
- Surveys / questionnaires of pupils / parents / carers / staff.

4. Scope of the Policy

This policy applies to all members of the academy community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of academy ICT systems, both in and out of the academy.

The academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

5. Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the academy:

6. Academy Advisory Committee

Academy Advisory Committee members are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Directors receiving regular information about e-safety incidents and monitoring reports. A member of the Academy Advisory Committee has taken on the role of monitoring Safeguarding. This includes E-Safety. E-Safety will be monitored through the Governors' Challenge and Support review schedule and will include:

- regular meetings with the e-Safety Lead
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Directors / Board / committee

7. Employees

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

All staff will be given access to the Academy Digital Learning policy and its importance explained.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff development in safe and responsible Internet use and on the academy Digital Learning policy will be provided as required.

8. Pupils

All pupils

- are responsible for using the academy digital technology systems in accordance with the Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras.

Pupils should also know and understand policies on the taking / use of images and on cyber-bullying and should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the academy's E-Safety Policy covers their actions out of school, if related to their membership of the school.

9. Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the academy in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / VLE and on-line / pupil records if applicable

Community Users who access school systems / website / VLE as part of the wider academy provision will be expected to sign a Community User AUA before being provided with access to school systems. (A Community Users Acceptable Use Agreement can be found in the appendices of the full academy Digital Learning policy.)

10. Teaching and Learning

The purpose of Internet use in Kinson Academy is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the academy's management information and business administration systems.

Internet use is a part of the curriculum and a necessary tool for staff and pupils.

The Internet is an essential element in 21st century life for education, business and social interaction. The academy has a duty to provide students with quality Internet access as part of their learning experience.

Pupils use the Internet widely outside the academy and will need to learn how to evaluate Internet information and to take care of their own safety and security.

11. Benefits of using the Internet in Education

- Access to worldwide educational resources including museums and art galleries.
- Educational and cultural exchanges between pupils via video conferencing.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration with support services, professional associations and colleagues.
- Improved access to technical support including remote management of networks and automatic updates.
- Access to learning wherever convenient.

12. Evaluating Internet content

If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the E-Safety Lead.
Academies should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

The evaluation of on-line materials is a part of every subject.

13. Managing Internet Access

The security of the academy ICT systems will be reviewed regularly.
Virus protection will be installed and updated regularly.
Security strategies will be discussed with the managed network provider. The network manager will review system capacity regularly (Westcoms network management).

14. Use of Email

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
Whole-class or group e-mail addresses should be used at Key Stage 2 and below for accessing Teams provision and communicating on this platform, as well as for limited access to education about emailing.
Excessive social e-mail use can interfere with learning and is not allowed.
The forwarding of chain letters is not permitted.

15. Published Content – Website

The contact details on the Web site should be the academy address, e-mail and telephone number. Staff or pupils' personal information will not be published.
The Principal or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
The Web site should comply with the academy's guidelines for publications including respect for intellectual property rights and copyright.
Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified without parental/carer permission.
Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
Written permission from parents or carers will be obtained before photographs of pupils are published on the academy Web site.
Pupils' work can only be published with the permission of the pupil and parents.

16. Social networking and personal publishing

Kinson Academy has a Service Level agreement with the South West Grid for Learning to block/filter access to social networking sites.

Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, academy, IM address, e-mail address, names of friends, specific interests and clubs etc.

Pupils are advised not to place personal photos on any social network space. They consider how public the information is and consider using private areas. Advice is given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name, academy, shopping centre.

Teachers are advised not to run social network spaces for students on a personal basis. Staff are given training and updates to aid protecting their digital identity on a regular basis.

Kinson Academy is aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

The E-Safety Lead will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

17. Emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the academy is allowed.

18. Personal data

Personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.

19. Internet Access

The academy will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
Primary pupils will not be issued individual e-mail accounts, but will be authorised to use a group/class e-mail address under supervision.

20. Risk Assessment

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The academy 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 an academy computer. Neither the academy nor BBC (for example the content of iPlayer) can accept liability for the material accessed, or any consequences of Internet access.

Methods to identify, assess and minimise risks will be reviewed regularly. The Principal will ensure that the E-Safety Policy is implemented and compliance with the policy monitored.

21. E-safety complaints

Complaints of Internet misuse will be dealt with by the E-Safety Lead.

Any complaint about staff misuse must be referred to the Principal.

22. Internet used across the community

The academy will be sensitive to Internet related issues experienced by pupils out of academy, e.g. social networking sites, and offer appropriate advice.

23. Communications Policy

Pupils will be informed that Internet use will be monitored.

Instruction in responsible and safe use should precede Internet access.

All pupils read, accept and sign our Academy Acceptable Use agreement.

24. Parental Support

Parents' attention will be drawn to the Academy E -Safety Policy in newsletters and on the academy Web site.

Child Protection / Safeguarding Designated Person / Officer
should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

(NB. it is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop. Due to this some schools choose to combine the role of Child Protection / Safeguarding and E-Safety). At Kinson Academy, the Principal and Inclusion Lead are responsible for Child Protection. The e-safety element has been delegated to Mr J Dighton, who our E-Safety Champion.