KINGSWOOD HOUSE SCHOOL

E-SAFETY POLICY

This Policy relates to the whole school including the Early Years Foundation Stage and during school clubs or activities outside the normal school day. The Policy is reviewed annually to ensure compliance with current regulations and law and **must** be read in conjunction with other relevant Kingswood House School policies.

Related Policies:

- **Pupils' Use of ICT, Mobile Phones and other Electronic Devices**
- **Use of Telephone, E-mail Systems and Internet**
- **IT Acceptable Use Policy**
- **Child Protection and Safeguarding Policy**
- **Low Level Concern Policy**
- **Anti-Bullying Policy**
- **Special Educational Needs, Learning Difficulties and Disabilities Policy**
- **Behaviour and Sanctions Policy**
- **Suspension and Exclusion of Pupils**

This list is not exhaustive.

Created by	**Sally Witts**
Reviewed by	**Katie Edwards**
Date	**16th September 2021**
Review date	**September 2022**

1. INTRODUCTION

1.1. This policy has been developed to ensure that all adults in Kingswood House School are working together to safeguard and promote the welfare of children and young people. This policy has to be ratified by the Governing Body.

1.2. **E-Safety is a safeguarding issue not an ICT issue**. All members of the school community must sign that they have read and understood the policy and guidelines confirming a duty of e-safety care at all times, to know the required procedures and to act on them. All staff receive training every three years in safeguarding, which is updated at the beginning of each term, and workshops are held annually on e-safety and cyberbullying to which our parents/carers are invited.

1.3. This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit using ICT, whilst minimising any associated risks. It describes actions that should be put in place to redress any concerns about child welfare and safety as well as how to protect children, young people and staff from risks and infringements.

1.4. The Headmaster or, in their absence, the authorised member of staff for e-safety, **Mr Ian Mitchell,** has the ultimate responsibility for safeguarding and promoting the welfare of pupils in their care.

1.5. This policy complements and supports other relevant school policies.

1.6. The purpose of internet use in school is to help raise educational standards, promote pupil achievement, and support the professional work of staff as well as enhance the school's management information and business administration systems.

1.7. The internet is an essential element in 21st century life for education, business and social interaction and the school has a duty to provide children and young people with quality access as part of their learning experience.

1.8. A risk assessment will be carried out, by **Mrs Pippa Webb**, before children and young people are allowed to use any new technology in the school and its settings.

2 ETHOS

2.1 It is the duty of the school to ensure that every child and young person in its care is safe. The same 'staying safe' outcomes and principles outlined in the Every Child Matters agenda apply equally to the 'virtual' or digital world. This expectation also applies to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

2.2 Safeguarding and promoting the welfare of pupils is embedded into the culture of the school and its everyday practice and procedures.

2.3 All staff have a responsibility to support safe e-safety practices in school.

2.4 All pupils need to understand their responsibilities in the use of all ICT at school.

2.5 E-safety is a partnership concern and is not limited to school premises, school equipment or the school day.

2.6 Bullying, harassment or abuse of any kind via digital technologies, social media or any platform, mobile phones or any other device will not be tolerated. Complaints of cyberbullying will be dealt with in accordance with the school's Anti-Bullying and Behaviour and Sanctions Policy.

2.7 Complaints related to child protection will be dealt with in accordance with the school's Child Protection and Safeguarding Policy.

3 ROLES AND RESPONSIBILITIES

3.1 The Headmaster of **Kingswood House School** will ensure that:

- All staff will receive E-Safety training.
- Staff understand that misuse of the internet may lead to disciplinary action and possible dismissal.
- A Designated Senior Member of Staff for E-Learning/Safety is identified **(Mr Ian Mitchell).** In this position he receives appropriate on-going training, support and supervision and works closely with the Designated Person for Safeguarding **(Mr Liam Clarke)**.
- All temporary staff and volunteers will be made aware of the school's E-Learning/Safety Policy and arrangements, and must sign the E-Policy Contract.
- E-Safety is an integral part of the safer recruitment and selection process of staff and will be included in their induction.
- The school's ICT systems are regularly reviewed with regard to security.
- The virus protection is regularly reviewed and updated.
- Regularly check files on the school's network.

3.2. The **Governing Body** of the school will ensure that:

- There is a senior member of the school's leadership team who is designated to take the lead on E-Learning/Safety within the school. **(Mr Ian Mitchell)**
- Procedures are in place for dealing with breaches of e-safety and security.
- All staff and volunteers have access to appropriate ICT training.

3.3 The Designated Senior Member of Staff for E-Learning/Safety **(Mr Ian Mitchell)** will:

- Act as the first point of contact with regards to breaches in e-safety and security.
- Liaise with the Designated Person for Safeguarding **(Mr Liam Clarke)** as appropriate.
- Ensure that ICT security is maintained.
- Attend appropriate training.
- Provide support and training for staff and volunteers on E-Safety as necessary.
- Ensure that all staff and volunteers understand and are aware of the school's E-Learning/Safety Policy.

Benefits of internet use for education

4.1 The internet is a part of the statutory curriculum and a necessary tool for staff and children and young people and benefits education by allowing access to world - wide educational resources.

4.2 Access to the internet supports educational and cultural exchanges between students world - wide and enables pupils to participate in cultural, vocational, social and leisure use in libraries, clubs and at home.

4.3 The internet supports professional development for staff through access to national developments, educational materials, good curriculum practice and exchange of curriculum.

4.4 The internet improves access to technical support, including remote management of networks, supports communication with support services, professional associations and colleagues as well as allowing access to, and inclusion in, government initiatives.

4.5 The internet offers opportunities for mentoring pupils and providing peer support for them and their teachers.

4.6 Internet use will be planned to enrich and extend learning activities and access levels will be reviewed to reflect the curriculum requirements and age of the children and young people.

4.7 Children and young people will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

4.8 Children and young people will be encouraged to question what they read and to seek confirmation of matters of fact from more than one source. They will be taught research techniques including the use of subject catalogues and search engines and encouraged to question the validity, currency and origins of information. Children and young people will also be taught that copying material is worth little without an appropriate commentary demonstrating the selectivity used and evaluating the material's significance.

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

5 MANAGING INTERNET ACCESS

5.1 Developing good practice in internet use as a tool for teaching and learning is essential. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the children and young people.

5.2 Pupils will be taught what internet use is acceptable and what is not and be given clear objectives for internet use. Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupil's age and maturity.

5.3 Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

5.4 If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Co-ordinator.

5.5 The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

5.6 Pupils will be taught to be critically aware of the materials they read as well as how to validate information before accepting its validity.

6 MANAGING E-MAIL

6.1 **No** Personal e-mail, texts, social media of any kind between staff and pupils to take place.

6.2 Staff **must use** their school or business e-mail address if they need to communicate with parents for school activity.

6.3 Pupils **must not** reveal details of themselves or others in any e-mail communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone.

6.4 Access in school to external personal e-mail accounts on school computers is forbidden.

6.5 Incoming e-mail with attachments from unknown authors should not be opened.

7 MANAGING WEBSITE CONTENT

7.1 Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.

7.2 All parents must sign the parental consent form for photographs of pupils to be used. If a child does not have consent then the school is responsible for ensuring that no photographs of the child are used. Consent is required from the pupils in Year 8 and above.

7.3 The point of contact on the school website will be the school address, school e-mail and telephone number. Staff or pupil's home information will not be published.

7.4 The Headmaster or nominated person will have overall editorial responsibility and ensure that all content is accurate and appropriate.

7.5 The website will comply with the school's guidelines for publications and parents/carers will be informed of the school policy on image taking and publishing.

7.6 Use of site photographs will be carefully selected so that pupils cannot be identified or their image misused.

7.7 The names of pupils will not be used on the website, particularly in association with any photographs.

8 MOBILE PHONES

8.1 Students are not permitted to bring mobile phones to school unless they have the permission of the Headmaster to use them for travelling and then they must be left in the school office (or in lockers for Years 7-11 during Covid precautions).

8.2 Authorised staff are permitted to take photographs with school cameras and/or school digital equipment for school purposes.

8.3 Staff personal mobile phones or tablets should not be used for photographs of school pupils.

9 SOCIAL NETWORKING AND CHAT ROOMS

9.1 The school will control access to moderated social networking sites and educate pupils in their safe use.

9.2 Pupils will not be allowed access to social networking sites on school technology e.g., My Space, Twitter, Facebook, Bebo, Instagram etc.

9.3 Pupils will be taught the importance of personal safety when using social networking sites and chat rooms.

9.4 Pupils will not be allowed to access public or unregulated chat rooms.

9.5 Pupils will only be allowed to use regulated educational chat environments and use will be supervised.

9.6 Newsgroups will be blocked unless an educational need can be demonstrated.

9.7 Staff will not exchange social networking addresses or use social networking sites to communicate with pupils.

10 FILTERING

10.1 The school will work in partnership with parents/carers, the Local Authority, the DfE and the Internet Service Provider to ensure systems to protect pupils and staff are reviewed and improved regularly.

10.2 If staff or pupils discover unsuitable sites, the URL **(address)** and content must be reported to the Headmaster or E-Safety Co-ordinator, **Mr Ian Mitchell.**

10.3 Any material the school deems to be unsuitable or illegal will be immediately referred to the Internet Watch Foundation (www.iwf.org.uk).

10.4 Regular checks by Senior Staff will ensure that the filtering methods selected are appropriate, effective and reasonable.

10.5 Filtering methods will be selected by the school and will be age and curriculum appropriate.

11 PHOTOGRAPHIC, VIDEO AND AUDIO TECHNOLOGY

11.1 All material is the copyright of the school and may not be reproduced unless written permission has been obtained by Headmaster.

11.2 Staff may use photographic or video technology, using school devices, to support school trips and appropriate curriculum activities.

11.3 It is not permitted to use photographic or video technology in changing rooms or toilets.

12 ASSESSING RISKS

12.1 Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and to develop good practice. The senior leadership team should be aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and allow a new route to undesirable material and communications.

12.2 In common with other media such as magazines, books and video, some material available through the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to international scale and linked nature of Internet content, it is not always possible to guarantee that unsuitable material may never appear on a school computer. Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences of Internet access.

12.3 Emerging technologies will be examined for educational use and a risk assessment will be carried out before use in school is allowed and methods to identify, assess and minimise risks will be reviewed regularly.

12.4 The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.

12.5 The Headmaster will ensure that the E-Safety Policy is implemented and compliance with the policy is reviewed and monitored annually.

12.6 Access to any websites involving gambling, games or financial scams is strictly forbidden and will be dealt with accordingly.

13 INTRODUCING THE POLICY TO PUPILS

13.1 Rules for responsible computer and internet access are signed by all pupils in the Prep Diary. Please refer to the policy on pupils' use of ICT, mobile phones and other electronic equipment.

13.2 Pupils will be instructed in responsible and safe use before being allowed access to the Internet and will be reminded of the rules and risks before any lesson using the Internet.

13.3 Pupils will be informed that internet use will be closely monitored and that misuse will be dealt with appropriately.

14 CONSULTING STAFF

14.1 It is essential that teachers and learning support staff are confident about using the internet in their work and should be given opportunities to discuss issues and develop appropriate teaching strategies:

- All staff are governed by the school's 'Child Protection and Safeguarding Policy' and 'E-Safety Policy' and their importance explained.
- Staff training in safe and responsible use of the internet will be provided as required.
- Staff will be aware that internet use will be monitored and traced to the original user. Discretion and professional conduct is essential.
- Senior managers will supervise members of staff who operate the monitoring procedures.

15 MAINTAINING ICT SECURITY

15.1 Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mails.

15.2 The ICT Manager will ensure that the system has the capacity to deal with increased traffic caused by Internet use.

16 DEALING WITH COMPLAINTS

16.1 Staff, children and young people, parents/carers must know how and where to report incidents. Concerns related to safeguarding issues must be dealt with through the school's Child Protection and Safeguarding Policy and Procedures.

16.2 The school's designated person for e-safety, **Mr Ian Mitchell**, will be responsible for dealing with complaints and any complaint concerning staff or pupil misuse of the internet must be reported to the Headmaster immediately.

16.3 Pupils and parents/carers will be informed of the complaints procedure.

16.4 Parents/carers and pupils will work in partnership with the school staff to resolve any issues.

16.5 As with drugs issues, there may be occasions when the school must contact the police. If appropriate, early contact should be made to discuss strategies and preserve possible evidence.

16.6 Sanctions for misuse may include any or all of the following:

- Interview/counselling by an appropriate member of staff
- Informing parents/carers
- Removal of internet access for a specified period of time, which may ultimately prevent access to files held on the system, including examination coursework.
- Referral to the police.

17 PARENTS/CARERS SUPPORT

17.1 Parents/carers will be informed of the school's E-Safety Policy which may be accessed on the school website.

17.2 Any issues concerning the internet will be handled sensitively to inform parents/carers without undue alarm.

17.3 Advice on filtering systems and appropriate educational and leisure activities including responsible use of the Internet will be made available to parents/carers.

17.4 Interested parents/carers will be referred to organisations such as Child Exploitation and Online Protection (CEOP).

17.5 A partnership approach will be encouraged with parents/carers and this may include practical sessions as well as suggestions for safe internet use at home.

18 COMMUNITY USE

18.1 School ICT resources may be increasingly used as part of the extended school agenda.