KINGSWAY COMMUNITY TRUST

KINGSWAY COMMUNITY TRUST

E-LEARNING/SAFETY POLICY

February 2019

E-Learning/Safety Policy

Date: February 2019

Review Date: Spring 2022

1 INTRODUCTION

1.1 This policy has been developed to ensure that all adults in the Kingsway Community Trust are working together to safeguard and promote the welfare of children and young people. This policy should be used in conjunction and with the Trust Safeguarding Policy

1.2 E-Safety is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.

1.3 This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained by exploiting the benefits and opportunities by 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 Executive Headteacher or, in their absence, the authorised member of staff for e-safety (the Head of School) has the ultimate responsibility for safeguarding and promoting the welfare of pupils in their care.

1.5 This policy should be used in conjunction and with reference to section 19 of the Safeguarding Policy - Preventing radicalisation and violent extremism.

1.6 This policy complements and supports other relevant school policies.

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

1.8 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 before children and young people are allowed to use new technology in schools and settings.

2. ETHOS

2.1 It is the duty of the school to ensure that every child and young person in it's 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 it's everyday practice and procedures.

2.3 All staff have a responsibility to support e-Safe practices in school and all pupils need to understand their responsibilities in the event of deliberate attempts to breach e-safety protocols.

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

2.5 Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will dealt with in accordance with the school's Anti-Bullying and Behaviour Policy.

2.6 Complaints related to child protection will be dealt with in accordance with the school's Safeguarding Policy.

3 ROLES AND RESPONSIBILITIES

3.1 The Executive Headteacher of Kingsway Community Trust will ensure that:

- All staff should be included in E-Safety training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal
- All staff are to read the Trust Staff IT Acceptable Use Policy and sign to acknowledge their understanding of the policy and give consent to adhere to it
- A Designated Senior Member of Staff for E-Learning/Safety is identified and receives appropriate on-going training, support and supervision and works closely with the Designated Person for Safeguarding.
- All temporary staff and volunteers are made aware of the school's E-Learning/Safety Policy and arrangements.
- A commitment to E-Safety is an integral part of the safer recruitment and selection process of staff and volunteers.

3.2. The Trust Board 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.
- Procedures are in place for dealing with breaches of e-safety and security and are in line with Local Authority procedures.
- All staff and volunteers have access to appropriate ICT training.

3.3 The Designated Senior Member of Staff for E-Learning /Safety will:

- Act as the first point of contact with regards to breaches in e-safety and security.
- Liaise with the Designated Person for Safeguarding as appropriate.
- Ensure that ICT security is maintained.
- Attend appropriate training.
- Provide support and training for staff and volunteers on E-Safety.
- Ensure that all staff and volunteers have received a copy of the school's Acceptable Use of ICT Resources document.
- Ensure that all staff and volunteers understand and aware of the school's E-Learning/Safety Policy.

- Ensure that the school's ICT systems are regularly reviewed with regard to security.
- Ensure that the virus protection is regularly reviewed and updated.
- Discuss security strategies with the Local Authority particularly where a wide area network is planned.
- Regularly check files on the school's network.

4 TEACHING and LEARNING

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 including art galleries and museums as well as enabling access to specialists in many fields for pupils and staff.

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 and administration data with the Local Authority and DfE.

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 Learning Facilitator.

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.

5.7 Support will be given to parents and carers to further their own understanding of the Internet and surrounding safety issues, so as to be able to keep their child safe online outside of school.

6 MANAGING E-MAIL

6.1 Personal e-mail or messaging between staff and pupils should not take place.

6.2 Pupils and staff may only use approved e-mail accounts on the school system and pupils must inform a member of staff immediately if they receive an offensive e-mail. Whole –class or group e-mail addresses should be used at KS1 and below.

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 may be blocked.

6.5 Excessive social e-mail use can interfere with learning and will be restricted.

6.6 E-mail should be authorised before sending to an external organisation just as a letter written on school headed note-paper would be.

6.7 The forwarding of chain letters is not permitted.

6.8 Incoming e-mail should be monitored and attachments should not be opened unless the author is known.

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 Photographs of pupils will not be used without the written consent of the pupil's parents/carers.

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 Executive Headteacher (delegated to the Personal Assistant) 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 to make sure pupils have photo consent.

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

7.8 Work will only be used on the website with the permission of the pupil and their parents/carers.

7.9 The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

7.10 Pupils will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Material which victimises or bullies someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented.

8. SOCIAL NETWORKING

SOCIAL NETWORKING AND CHAT ROOMS

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

8.2 Pupils will not access social networking sites eg 'Instagram', 'Facebook' or 'Snapchat'.

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

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

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

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

8.7 Pupils will be advised to use nick names and avatars when using social networking sites.

8.8 Staff will not exchange social networking addresses or use social networking sites to communicate with pupils (including ex-pupils) and parents, including those who are family and friends.

8.8a Staff members must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

8.9 Should special circumstances arise where it is felt that communication of a personal nature between a member of staff and a pupil is necessary, the agreement of a senior manager should always be sought first and language should always be appropriate and professional.

8.10 The school will use Social Media as appropriate to further enhance the reputation of the school, to showcase its achievements and as a means of communication with parents and carers.

9 MOBILE PHONES

9.1 Mobile phones will not be used during lessons or formal times in school. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden and will be dealt with in accordance with the school's Anti-Bullying and Behaviour Policies. Pupils are not allowed to use mobile phones in school and when needed for the journey to school, this should be agreed with the office and the phone stored there during the day.

9.2 Staff are not to take photographs or videos of children on their personal mobile phones unless authorisation has been given. This will be under certain circumstances i.e weekend residential trips. If photographs or videos are taken on residential trips, the images should be downloaded to the school IT system immediately on return to school, and deleted from personal devices. In school, if photographs or videos need to be taken they must be done so on a school issued camera, photographic or video recording equipment.

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. The 'safe search terminology' within our e-safety policies has been updated to include any terminology that may be considered relevant to the PREVENT criteria. Our Barracuda filtering generates an email to the ICT Network Manager regarding suspicious search queries. This will pick up if student or staff have tried to search for anything that may be deemed as suspicious.

Our Barracuda filtering works in two ways when a user tries to search or access internet resources.

a) It checks against the built-in database which is an education specific list of more than one billion entries. This database is maintained and updated on an on-going bases by Barracuda.

b) In the unlikely event that it gets past the Barracuda database of words, then it also checks it against the schools own specific database of words that is created by the trust. This is maintained by the trust and includes any terminology that may be considered relevant to the PREVENT criteria: for example "al qaeda" or "suicide bomber". This list is not exhaustive, but has been compiled in conjunction with key agencies recommendation and is regularly monitored and updated by SLT."

10.2 If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the IT Network Manager and the Executive Headteacher.

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 in conjunction with the LA and will be age and curriculum appropriate.

11 AUTHORISING INTERNET ACCESS

11.1 All staff including staff not directly employed by the school must read and sign the school's 'Staff IT Acceptable Use Policy' before using any school ICT resources.

11.2 The school will maintain a current record of all staff and pupils who are allowed access to the school's ICT systems.

11.3 The school will maintain a record of pupils whose parents/carers have specifically requested that their child be denied internet or e-mail access.

11.4 Parents/carers will be asked to sign and return the school's form stating that they have read and understood the school's 'Acceptable Use' document and give consent for their child to access ICT resources.

11.5 Staff will supervise access to the internet from the school site for all pupils.

12 PHOTOGRAPHIC, VIDEO AND AUDIO TECHNOLOGY

12.1 When not in use all video conferencing cameras will be switched off and turned towards the wall.

12.2 It is not appropriate to use photographic or video technology in changing rooms or toilets.

12.3 Staff may use photographic or video technology to capture to support school trips and appropriate curriculum activities.

12.4 Audio and video files may not be downloaded without the prior permission of the network manager.

12.5 Pupils must have permission from a member of staff before making or answering a videoconference call or making a video or audio recording in school or on educational activities.

12.6 Videoconferencing and webcam use will be appropriately supervised for the pupil's age.

13 ASSESSING RISKS

13.1 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.

13.2 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.

13.3 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.

13.4 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.

13.5 The Executive Headteacher will ensure that the E-Safety Policy is implemented and compliance with the policy is monitored.

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

14 INTRODUCING THE POLICY TO PUPILS

14.1 Rules for Internet access will be posted in all rooms where computers are used.

14.2 Responsible Internet use, covering both school and home use, will be included in the PSHE curriculum.

14.3 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.

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

15 CONSULTING STAFF

15.1 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 terms of the school's 'Staff IT Acceptable Use Policy' and will be provided with a copy of this policy and it's importance explained.
- Staff development 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.

16 MAINTAINING ICT SECURITY

16.1 Personal data sent over the network will be encrypted or otherwise secured.

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

16.3 The IT Network Manager will ensure that the system has the capacity to deal with increased traffic caused by Internet use.

17 DEALING WITH COMPLAINTS

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

17.2 The school's designated person for e-safety will be responsible for dealing with complaints and any complaint concerning staff or pupil misuse of the internet must be reported to the Executive Headteacher immediately.

17.3 Pupils and parents/cares will be informed of the complaints procedure.

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

17.5 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.

17.6 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.

18 PARENTS/CARERS SUPPORT

18.1 Parents/carers may receive a copy of this policy on request.

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

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

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

18.5 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.

20. Virtual Learning Environments

20.1 Seesaw, a learning platform which is in use at Ladybarn Primary, Green End Primary and Cringlebrook Primary, across all year groups respectively, provides a range of features for the delivery, support, administration and participation in teaching and learning activities. Seesaw has features which include content delivery and collaboration between teacher and learners, such as:

- Content creation or upload;
- Lessons;
- Discussion forums;
- Assignments;
- Quizzes; and
- Monitoring of users' online activity in ‘grade-books’.
-

20.2 The following conditions are made for our learning platform use by any authorised user. For the purposes of this policy, an authorised user is any member of staff, pupil or parent who has been given access to the system by the ICT Learning Facilitator, acting on behalf of the Executive Headteacher.

- Not use Seesaw for anything else other than for the purposes of teaching, learning and research.
- Not use Seesaw for personal commercial use, for example marketing.

- Not use Seesaw for uploading, storing, viewing or transmitting any material which is (or may be considered to be) defamatory, inflammatory, discriminatory, obscene, offensive, illegal, personal, sensitive or confidential.
- Not misrepresent the school or bring it into disrepute in any way through the use of the VLE.
- Be responsible for moderating discussion forums which they may have created and participate in.
- Always act in a professional manner. Be polite and courteous to others when using Seesaw. These learning platforms are not to be used to bully, slander, or harass any other persons.
- Not plagiarise in submitted postings or assignments.

20.3 Additional Responsibilities and Data Protection

Authorised users shall:

- Look after their own username and password.
- Change their password if they suspect it to be compromised.
- Keep physical access to the VLE secure. For example, do not login to the VLE and then leave the computer unattended.
- Not attempt to gain unauthorised access to any part of the VLE.
- Report any discovery or suspicion of use of the VLE that contravenes any of the conditions of use in this document, whoever it might be perpetrated by or involve, including attempted or actual unauthorised access
- Not post material which contains viruses or other programs which may disrupt the school's systems.
- Not upload private, confidential or sensitive material unless this is authorised by school management.
- Keep their own data up-to-date and secure.
- Understand that Kingsway Trust will not take responsibility for any loss of information, which has been posted on the VLE, once users cease to be formally associated with the school.

20.4 Breach

- The senior member of staff in charge of the VLE is the staff member with responsibility for ICT. This is delegated to the IT Network Manager.
- At first instance the IT Network Manager will be informed of any issues. Technical Issues will be dealt with by liaising with suppliers and the IT Network Manager. Non-technical issues will be reported to the Executive Headteacher, who will deal with it at her discretion, and sanctions may include restricting or removing VLE access, in addition to other school systems which may be invoked on a temporary or permanent basis. In very serious cases other agencies may be called in, including but not limited to Child Protection Services, Law Enforcement agencies, Social Services or any other appropriate agencies.

Issue Status

Date	Issue	Date approved by Trustees	Review date
February 2016	Version 1- February 2016		Spring 2019
February 2019	Version 2 – February 2019	1st April 2019	Spring 2022
Updated for GDPR and social media detail			

Appendix A

Student Acceptable Use Policy & Code of Conduct

I know that I must use the computers safely

- I know that the school can remotely monitor what I do on the computers.
- I will treat my username and password confidentially – I will not let anyone else use it, and I will not use theirs.
- I will be aware of my personal safety when I am communicating online, and will not share personal information about myself or others.
- I will tell a teacher immediately about any unpleasant or inappropriate material or messages on the computer, or anything that makes me feel uncomfortable when I see it.
- I understand that the school will look after me and my classmates and can help if anything happens online – even if I am using a computer at home.

I know that I must use the computers responsibly

- I understand that the computers are here for school work, and I will only play games on them or use them for personal use if I have permission.
- I will only upload pictures or videos from inside the school if I have permission.
- I understand that the school's security and Internet filter is there to protect me. If I need access to a blocked website, I will ask my teacher.
- I will only download music or videos onto the computer if it is related to my school work.
- I understand that I must not download or display inappropriate pictures or other material from the Internet.

I know that I must help look after the computers

- If I have a problem with my computer, I will tell a teacher immediately so that the problem can be fixed – I won't leave it broken for the next person.
- I will only use programs that are already on the school computer. If I need a new program, I will ask my teacher - I won't try to install it myself.
- I will not try to connect my own computer or mobile phone to the network.

- I will only change settings on the computer if I am allowed to do so – I won't try to change anything that might cause the computer to go wrong.

- I know that food and drink is not allowed in the computer rooms, and that I should not eat or drink around any computer.

I know that I must respect others when using the computers

- I will always treat others the same way I would want them to treat me – just as I would when not using the computers. I will not use the computers to harass or bully anyone.
- I will be polite online, and I will not use strong, aggressive, or inappropriate language. I appreciate that others may have different opinions.
- I will not take or distribute pictures or videos of anyone without their permission.