KENILWORTH SCHOOL
& SIXTH FORM

Safeguarding in a Digital World
E-Safety Policy

APRIL 2017

POLICY DETAILS	
Date of policy:	April 2017
Date of review:	April 2018

Member of staff responsible for overseeing that this policy is implemented and regularly reviewed:

Richard Garratt

1

Contents

1.0 Aims

1.1 The aims of this policy are:

- To enable governors to accept responsibility in ensuring that computer systems and the Internet within school are used in a respectful manner by all staff and that any occasion where there is cause for concern allow this to be treated seriously and investigated in a fair manner.
- To allow staff to access and the use ICT facilities including the Internet for educational purposes and limited personal use (see above statement).
- To clarify to staff expectations when using the school computer systems and the Internet.
- To encourage an environment that recognises the advantages of using computers and the Internet.
- To give staff and students the right to be safe and happy in school using the computer system, and to be protected.

2.0 School acceptable user policy:

2.1 Before accessing computers within school a signed declaration form that this policy has been read will be required. (See page 9 – Appendix 1).

2.2 When accessing computers within school we expect:

- The individual user to act responsibly. This includes ensuring your password remains secret and not allowing any other person access to your user area.
- The individual user to respect the property - this includes both hardware and software.
- The school at any time can examine any files held on its system. Senior Leadership Team (SLT) and senior ICT Technicians can monitor staff areas and delete/restrict access where it feels appropriate.

2.3 The governing body recognises the use of its ICT and communications facilities as an important resource for teaching, learning and personal development and as an essential aid to business efficiency. It actively encourages staff to take full advantage of the potential for ICT and communications systems to enhance development in all areas of the curriculum and school administration. It is also recognised by the governing body that along with these benefits there are also responsibilities, especially for ensuring that students are protected from contact with inappropriate material.

2.4 In addition to their normal access to the school's ICT and communication systems for work-related purposes, the governing body permits staff limited reasonable personal use of ICT equipment and e-mail and Internet facilities during their own time subject to such use:

- not depriving students of the use of equipment and/or

- not interfering with the proper performance of the staff member's duties

2.5 Whilst the school's ICT systems may be used for both work-related and for personal use, the governing body expects use of this equipment for any purpose to be appropriate, courteous and consistent with the expectations of the governing body at all times.

2.6 The school operates a ‘Policy Central’ security system which monitors images and wording used by both students and staff. If inappropriate text or images are detected the software takes a screen shot which is logged and highlighted to the ICT technicians who monitor the network usage. The technicians will then notify SLT for appropriate action.

2.7 The following are **NOT** permitted when using the school computer system (or using devices provided by the school such as net books, Laptops or iPad’s etc. out of school).

- Sending/displaying offensive messages, images or sounds.
- Using obscene language in any form of communication.
- Using harassing or threatening language in any form of communication e.g. The sending of emails.
- Deleting files or folders that were not created by themselves without permission of the originator.
- Sending confidential or sensitive information to those who are not authorised to receive it.
- Damaging computer hardware.
- Damaging computer software (e.g. knowingly bringing in a virus on a device and introducing it onto the school system).
- Violating copyright law.
- Sharing passwords to allow access on to the school system.
- Allowing others to use your computer under your own log on.
- Knowingly accessing material considered unsuitable.
- Bringing into school material considered unsuitable and /or introducing it on the school system.
- Theft of equipment.
- Downloading unsuitable files onto the school system.
- Use proxy's within school to access other Internet sites that are blocked by the network manager.
- Publish images of students from school without the permission of a parent/career first.
- Use personal equipment such as cameras, phones etc. to take images/video of students.
- Communicate with students through means outside of the school facilities such as personal email accounts, social networking sites, personal mobile phones etc.

2.8 Staff should be aware that the computer network is monitored by systems within school. School devices such as netbooks and laptops etc. that are able to access the Internet at home will log web pages that individuals have visited whilst at home

- these logs cannot be deleted by the user. School monitoring systems will analyse these logs when connected back onto the school network.

3.0 Social Network sites

3.1 Staff should ensure that their personal social network pages are sufficiently protected so as not to allow any parents or students to access personal information, comments or photographs. It is recommended that Facebook pages are set to 'Friends' thus preventing them being viewed by the general public.

3.2 Staff must not accept current students on roll as friends on 'Facebook', Instagram, Whatsapp, Twitter or any other form of social media as this can leave staff open to false claims and put them in a vulnerable position. Relationships between staff and students are excellent and we want to maintain this, and ensure that an appropriate distance between staff and students is adhered to. Staff should also not signpost students to their 'You Tube' accounts**.**

3.3 Equally, staff should not use social networks sites or the internet or personal blogs etc. in such a manner that the content is derogatory towards colleagues or brings the school into disrepute.

3.4 School respects a staff member's or student's right to a private life but it must also ensure that confidentiality and its reputation are protected. It therefore requires staff and students using social networking websites to:

- refrain from identifying themselves as working for the School;
- Refrain from placing any work related issue or material that could identify an individual who is a student or colleague, which could adversely affect the school;
- ensure that they do not conduct themselves in a way that is detrimental to the School; and
- take care not to allow their interaction on these websites to damage working relationships between colleagues and students.

4.1 Student Data

4.2 Any student data being transferred by a member of staff between school and home should, either be encrypted, or stored on a password protected memory device and should never be divulged to a third party. If a member of staff does not possess a password protected memory stick the use of school emails or 'drop boxes' are permitted (as long as the password is not shared amongst other users).

4.3 Staff must not publish student data regarding the progress of students outside of the school systems in the interest of data protection. Staff should ensure that any marking of students' work is undertaken in a confidential manner and marks or feedback for an individual student must not be accessible to other students or users on the system.

4.3 Any assessment or personal data relating to individual students will only be made available to their own families.

5.0 Student Email

5.1 All students will be provided with a school email account. Staff should only communicate with students through their school issued email system.

5.2 Access to the school network is provided for students to carry out recognised schoolwork and extra-curricular activities, but only on the condition that they agree to follow the schools E-Safety policy. A separate document for students entitled ICT Student Code of Conduct provides full details.

6.0 Staff Email

6.1 All staff will be provided with a school email account. Personal usage for this email account is permitted by the school. The email system is not to be used for the creation or distribution of any type of offensive or disruptive content. If you receive any messages with this type of content then you should report the matter immediately to SLT.

6.2 Staff should have no expectation of privacy in anything they create, store, send or receive on the school email system and the school may monitor email messages without any prior notice. Staff should also not forward any confidential messages or attachments to other establishments without permission.

6.3 If a member of staff is found to be in breach of the email policy rules, this could result in disciplinary action.

7.0 E-Safety for students

7.1 All students and their parent/carer must sign an acceptable ICT User agreement (copy contained in Student School E-Safety Policy/ICT Code of Conduct document). (See pages 10 -11 – Appendix 2).

7.2 There is an underlying assumption that students have both understanding and application of “safety”. Students need to understand that rules given to them must be followed. Students need to learn safety rules in a way that does not frighten them and which gives them confidence to know what to do in certain situations. Students need to understand that certain rules will change and develop as they get older.

8.0 E-Safety for students with additional needs

8.1 There are certain aspects of the above that are particularly challenging for students with additional needs and students who we may consider to be vulnerable in this learning context. Students will clearly have individual needs that will present different issues when teaching E-Safety but some common difficulties may be:

- They may be still developing their social understanding of safety and so may relate better to strategies used with younger students.

- They are likely to find it hard to apply the same rules in different situations. Most safety principles rely on students being able to explain what happened or to ask for help.
- Some students may have poor recall and difficulties with learning through experience.

8.2 The SENCO should coordinate advice between ICT specialist and support staff. This should take the form of very student focused strategies that would apply to a student with specific needs that would need to be available to all staff implicated in Internet use with that student. Alternatively, whole school approaches could take into consideration strategies that would support the needs i.e. specific choices of visual support to remind students of the rules.

9.0 Appropriate strategies

9.1 We will ensure that the use of Internet derived materials by staff and by students complies with copyright law, students will be made aware of plagiarism and issues relating to work research being undertaken for coursework. Staff and students will be trained to become critically aware of the materials they read and shown how to validate information before accepting its accuracy. Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

9.2 Staff must not publish data regarding their progress in the interest of data protection. Staff should ensure that any marking of students' work is undertaken in a confidential manner and marks or feedback for an individual student must not be accessible to other students or users on the system.

10.0 Digital Images

10.1 The school record of parental permissions granted/not granted must be adhered to when taking images of our students. A list is published to all staff on a termly basis, but can also be obtained from the data office.

10.2 Under no circumstances should images be taken using privately owned equipment without the express permission of the Headteacher.

10.3 Where permission is granted the images should be transferred to school storage systems (server or disc) deleted from privately owned equipment at the earliest opportunity.

10.4 Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

11.0 Sanctions

11.1 The misuse of school's computer systems by a member of staff will be reported to the Headteacher. By failing to follow the acceptable user policy you could be subject to disciplinary action. This could include a warning, suspension, dismissal, referral to governors and in the event of illegal activities the involvement of the police.

12.0 Other Related Policies

12.1 The E-Safety Policy works in conjunction with other policies including:

- Behaviour and Rewards
- Child Protection
- Curriculum policies
- Data Protection Policy
- Student ICT Code of Conduct

13.0 Approval and Review

13.1 This Policy was ratified by Governors on 27th April 2017. It will be reviewed again in April 2018, unless Local Authority or School needs dictate an earlier review.

APPENDIX 1

Kenilworth School
& Sixth Form

Safeguarding in a Digital World - E-Safety Policy

Acceptable ICT User agreement

I have read the '*Safeguarding in a digital world - E-Safety Policy*' and agree to adhere to the points under each of the individual headings.

Subject area: ____

Name (print): ____

Signature: ____

Date: ____

Please complete this form and return to Richard Garratt, Assistant Head

APPENDIX 2

KENILWORTH SCHOOL – STUDENT ICT ACCEPTABLE USER POLICY

Access to the school network is provided for you to carry out recognised schoolwork and extra-curricular activities, but only on the condition that you agree to follow the schools e-safety policy.

General

- Never have drinks or food near the computers
- Never tell your password to anyone else or let them use your account.
- Never use another person's account.
- Use strong and sensible passwords – at least 8 letters and a mixture of numbers and lower and upper case numbers
- Never install or run any programs on a school computer except official school software
- Always log off the computer when you have finished.
- Only use a printer for school-related work and activities and do not waste paper
- Never try to adjust or move computer equipment
- Remember - the school staff can automatically look at your work and check what you are doing at any time

The Internet and E-mail

- The school monitors all the websites you go on and all the emails you send
- Remember that, if you use a banned word, this will be detected and recorded.
- Never send, display, access or try to access any obscene or offensive material.
- Never send, display, access or try to access any materials relating to extremism, terrorism or violence (unless for a legitimate reason connected to learning)
- Never swear, use vulgarities, or any other inappropriate or offensive language.
- Never harass, insult or attack others through electronic media.
- If you receive an offensive email tell a member of staff straight away.
- Never copy and make use of any material without giving credit to the author. This would be plagiarism and breaking copyright rules.
- Never give out any personal information, such as you home address or personal phone numbers
- Check with a member of staff before opening unidentified e-mail attachments or completing questionnaires or subscription forms.
- Social networking sites and newsgroups are normally blocked.
- Only use schools email accounts on the school system especially when emailing your teacher.
- Never arrange to meet anyone you have met online without specific permission.
- **Never publish anything (in or out of school) on the internet (Facebook, Youtube, etc) that is rude or disrespectful to the school.**

Some behaviour is also against the law – this includes:
Never attempt to by-pass any security systems either systems in school or outside school (Computer Misuse Act)

- Never look at files which are nothing to do with you, especially other people’s files (Computer Misuse Act) and data (Data Protection Act)
- Never copy or install software without permission (Copyrights Designs and Patents Act)
- Never copy other people’s work without giving them credit (Copyrights Designs and Patents Act)
- Never use any personal photos without permission and consent (Data Protection Act)
- Never send obscene pictures (Child Protection Act, Obscene Publications Act)

Kenilworth Sports College

Student School E-Safety Policy

Please return this sheet to your form tutor.

I have read the student E-Safety policy and agree to abide by its rules.

Form group: __________

Student Name: _______________________ Signature: _____________________

Parent / Guardian Name: __________________ Signature: __________________

Date: ____________________

From time to time it is possible that Kenilworth School may publish images for an educational purpose of students within newsletters, local press or the school website. Certain departments also need to video students as part of their subject syllabus; **in some instances it is a requirement of the examination board.**

Please be assured that all videos and photographs will be sensitively taken and appropriate at all times.

1) Please indicate below whether you give permission for child's image to be used in **Internal school publications / notice boards etc**:

I do give permission □ I do not give permission □

2) Please indicate below whether you give permission for child's image to be used in **External school publications**:

I do give permission □ I do not give permission □

3) Please indicate below whether you give permission for child's image to be used in **subject area videos**:

I do give permission □ I do not give permission □