Kenn and Kenton Federation

Computing/E-Safety Policy.

STATEMENT OF SAFEGUARDING CHILDREN

At Kenn and Kenton Federation, our school communities have a duty to safeguard and promote the welfare of children who are our pupils. We take this duty very seriously. This means that we have a Safeguarding Children and Child Protection Policy and Procedures in place to which we refer.

All staff including our volunteers and supply staff must ensure that they are aware of our procedures. Our Policy is on the school website. Sometimes we may need to share information and work in partnership with other agencies when there are concerns about a child's welfare. We will always ensure that our concerns about our pupils are discussed with their parents/carers first unless we have reason to believe that this is not in the child's best interests.

Our Designated Child Protection Officer is: Amanda Somerwill, **Executive HEADTEACHER**

Our Designated Governor for Child Protection is: Joe Baxter

Writing and reviewing the e-safety Policy

The Federation will appoint the computing coordinator as e-safety coordinator.

This policy will be reviewed annually and consideration given to new technologies and guidance.

Introduction

ICT in the 21st century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. Information and Communications Technology covers a wide range of resources, including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the Internet technologies children and young people are using both inside and outside the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging • Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Reviewed by Teaching & Learning Committee – Summer 19
Review due: Summer 20

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, is not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies. Some of the dangers they may face include:

• Access to illegal, harmful or inappropriate images or other content

• Unauthorised access to / loss of / sharing of personal information

• The risk of being subject to grooming by those with whom they make contact on the Internet.

• The sharing / distribution of personal images without an individual's consent or knowledge

• Inappropriate communication / contact with others, including strangers

• Cyber-bullying

• Access to unsuitable video / Internet games

• An inability to evaluate the quality, accuracy and relevance of information on the Internet

• Plagiarism and copyright

• Illegal downloading of music or video files

• The potential for excessive use which may impact on the social and emotional development and learning of the young person.

At Kenn and Kenton Federation we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom.

The schools' Internet access is provided through the South West Grid for Learning (SWGfL), which is designed for pupil use and includes filtering appropriate to the school. The system is managed by the South West Grid for Learning.

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The schools 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.

Teaching and Learning.

Internet use will enhance learning

• Pupils are taught what Internet use is acceptable and what is not, and given clear objectives for Internet use

• Pupils are educated in the effective use of the Internet and in research, including the skills of knowledge location, retrieval and evaluation

• Pupils are shown how to publish and present information to a wider audience

Pupils will be taught how to evaluate Internet content

• The schools will ensure that the use of Internet derived materials by staff and pupils complies with copyright laws

• Pupils will be taught the importance of cross-checking information before accepting its accuracy

• Pupils will be taught how to report unpleasant Internet content

E-mail

- Pupils may only use approved e-mail accounts on the schools system
- Pupils must immediately tell a teacher if they receive offensive email
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mails should be treated as suspicious and attachments not opened unless the author is known.
- E-mails from pupils to external bodies are to be monitored and controlled by teachers and support staff.
- The forwarding of chain letters is not permitted.

School website

• The school websites are updated and maintained by all permanent school staff, authorised persons, the chair of governors and the clerk

• No personal information about any member of the school community will be published on the website

• Written permission from parents or carers will be obtained before photographs of pupils are published on the website

• Pupil image files will refer to the pupil by first name only

• Parents are clearly informed of the school's policy on image taking contained in our Intimate Care Policy

Networking

Educational networking sites, such as Google Classroom will be used under close supervision in the schools, where the content of discussions and forums will be the responsibility of the adult supervising them. The Federation's Twitter accounts are used by staff only. All staff will be made aware of the personnel policy on the use of social media.

The use of online chat rooms, instant messaging services and text messaging will not be allowed in school until the Federation community agrees that these technologies can be supervised or monitored in a way that will guarantee the safety of pupils. Thus unauthorised social networking sites and newsgroups will be blocked and filtered, except for teaching sessions on safer use, when filtering will be lifted on specific sites for limited time periods.

We do, however realise that some pupils do use such sites outside school and the schools will educate pupils on their safe use.

• Pupils are advised never to give out any personal details that might identify them or their location • Pupils are advised not to place personal photos on any social network space

• Pupils are advised on security and encouraged to set passwords, and maintain profiles to maximum privacy and deny access to unknown individuals

• Pupils are advised never to agree to meet someone they have met on a social networking site

• If pupils have any concerns about social networking sites or chat rooms, they are advised that they must tell an adult

Managing filtering

The school will work with Devon County and SWGfL to ensure systems to protect pupils are reviewed and improved. If staff or pupils come across unsuitable online materials the site must be reported to the Computing Co-ordinator.

Senior staff, Computing Co-ordinator and ICT support will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

Emerging technologies will be examined for educational benefits and a risk assessment will be carried out before use in school is allowed.

Managing video conferencing and webcam use

Videoconferencing will use the educational broadband network to ensure quality of service and security.

Pupils must ask permission from the supervising teacher before making or answering a videoconference call and must be appropriately supervised.

Mobile Phones

• The use of mobile phones will not be permitted during lessons or formal school time by staff or pupils. This excludes occasions when staff may need to use mobile phones, for example on school trips or activities off-site, or as part of a demonstration in a lesson.

• Staff may use their mobile phones in the staff room or outside formal school time.

• The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden

• Staff should not use their own mobile phone camera to take photographs of children

Education

E-Safety education will be provided in the following ways:

• A planned e-safety programme will be provided as part of Computing / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school using a range of resources including www.thinkuknow.co.uk.

• Key e-safety messages should be reinforced as part of a planned programme of assemblies / classroom based activities

• Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

• All staff have access to guidance on e-safety and progression in ICT (see e-sense document)

Reviewed by Teaching & Learning Committee – Summer 19
Review due: Summer 20

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

• in lessons where Internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

• Where pupils are allowed to freely search the Internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

• It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, and discrimination) that would normally result in Internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

• Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

• Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 2018 and the Federation's Data Protection Policy.

Cyber Bullying

Cyber bullying is when the Internet, mobile phones or electronic devices are used intentionally to hurt or embarrass another person. As with any other type of bullying, cyber bullying only occurs if a person is repeatedly tormented, threatened, harassed, humiliated, embarrassed, or otherwise targeted by another person using digital technology.

Cyber bullying will not be permitted by the schools. This is as important to the schools as any other type of bullying and this is an integral part of the Federation Behaviour & Anti-bullying Policy.

Internet Access

Authorising Internet access

• All pupils (from Yr 3 upwards) read and sign the Responsible Internet Use form before using the Federation ICT resources. Pupils will be reminded annually of the safety rules at the beginning of the autumn term.

• The schools will maintain a log of all non-school members who are granted access to the school ICT system

At Foundation and Key Stage One, access to the Internet will be by adult demonstration with supervised access to specific, approved online materials.

Managing Internet Access

• The Federation's ICT system security will be reviewed regularly

• All pupil Internet access will be supervised by an adult

Reviewed by Teaching & Learning Committee – Summer 19
Review due: Summer 20

• The schools will take reasonable precautions to prevent access to inappropriate material, including radicalisation and related extremist content (please refer to our Preventing Radicalisation Policy). 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 a computer connected to the school network.

• Raw image searches are discouraged when working with pupils

• If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research

• All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources

• Staff and pupils are aware that school-based email and Internet activity can be monitored and explored further if required

• If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the ICT coordinator or teacher as appropriate

• It is the responsibility of the schools, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines

• Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software

Passwords and Password security

- Always use your own passwords to access computer based services
- Make sure you enter your personal password each time you logon. Do not include passwords in automated logon procedures.
- Make sure to log out of password protected Internet sites.
- Staff are advised to change their passwords regularly

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with anyone particularly friends. Staff and pupils are regularly reminded of the need for password security.

School IT Equipment including Portable and Mobile IT equipment and Removable Media.

• As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you

• All ICT equipment issued to staff is recorded to include serial numbers as part of the school's inventory and will be security marked

• Personal or sensitive data including photos of pupils should be stored on the terminal server and not on desktop PCs

• Staff must ensure that all school data is stored on the school's network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted

• All ICT equipment should be kept physically secure and will be covered for insurance purposes

Reviewed by Teaching & Learning Committee – Summer 19
Review due: Summer 20

Safe use of Images

Taking of Images and Film.

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. Parents will be reminded of this before all school\Federation events

Please refer to our Intimate Care Policy for details of the federation policy and procedures on the use of photography and videos for parents/carers.

All parents/carers are asked to read and sign our guidelines on the use of photography/video when their child starts school.

Yearly parents will be asked to sign and return photographic\video permission consent slips.

Parental Involvement

We believe it is essential for parents/carers to be fully involved with promoting e-safety both in and outside school, and also to be aware of their responsibilities. We regularly consult and discuss e-safety with parents/carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/carers attention will be drawn to the Federation E-Safety Policy in newsletters, and on the school website

- Parents/carers are asked to read and sign the acceptable use agreements on behalf of their child on admission to school. Pupils will be reminded annually of the safety rules at the beginning of the autumn term

Community Use of the Internet

The school will liaise with community users to establish acceptable use of the Internet.

Communicating the policy

Acceptable use\ e-safety rules will be displayed in classrooms and the computer suite

Staff and pupils will be informed that the network and Internet use will be monitored and appropriately followed up

A program of training will be part of the curriculum for the pupils

All staff will receive training in e-safety, with regular updates, and the importance explained.

Staff who monitor IT and manage the filtering systems will be supervised by senior management and work to clear procedures for reporting issues.

Reviewed by Teaching & Learning Committee – Summer 19
Review due: Summer 20

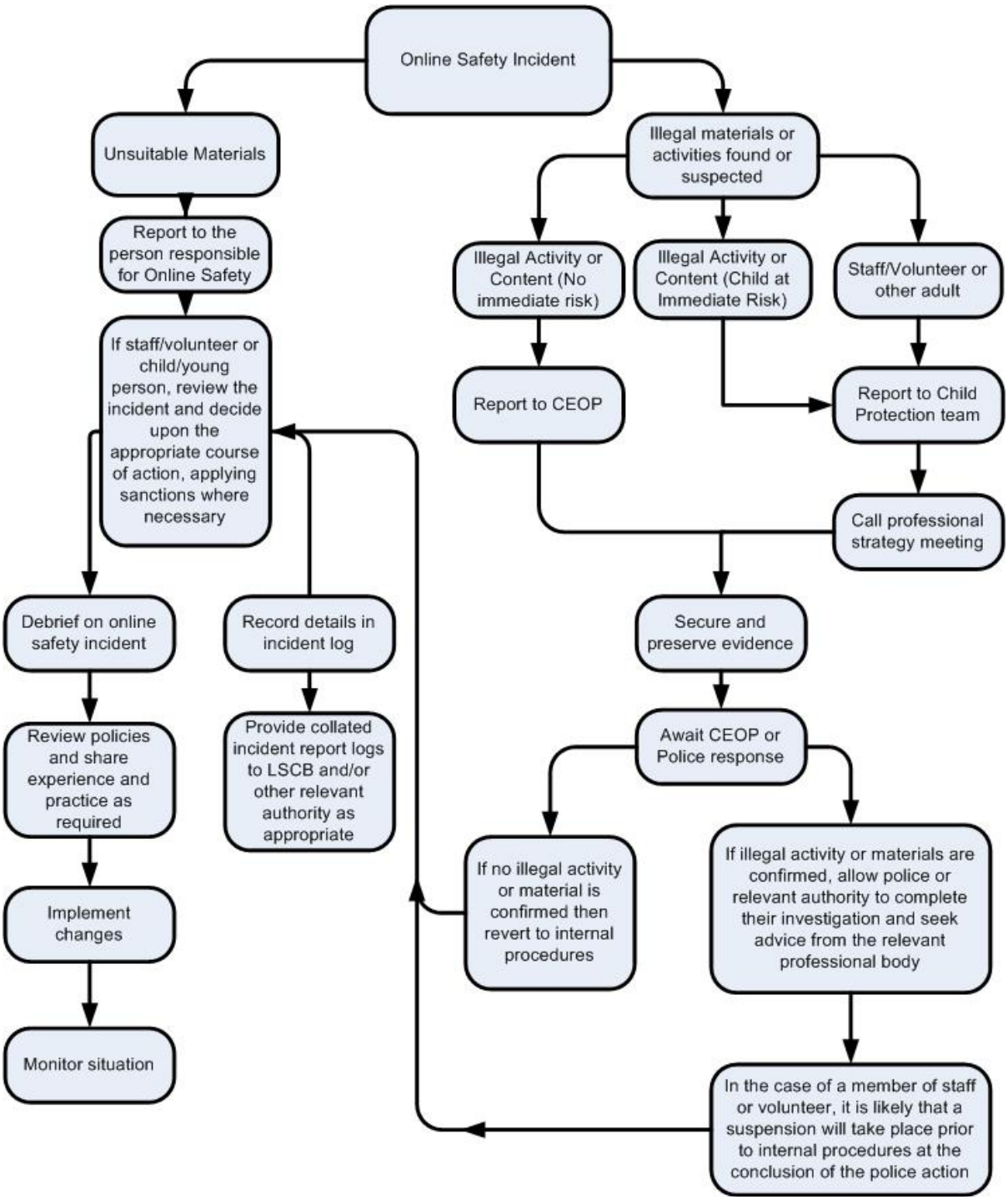
Responding to incidents of misuse

It is hoped that all members of the federation community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse: If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

Responding to incidents of misuse – flow chart



Appendices 1

Acceptable use Policy for children

Student / Pupil Acceptable Use Policy Agreement Template – for younger pupils (Foundation / KS1)

This is how we stay safe when we use computers:

Reviewed by Teaching & Learning Committee – Summer 19
Review due: Summer 20

I will ask a teacher or suitable adult if I want to use the computers

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will take care of the computer and other equipment

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Kenn and Kenton Federation

Responsible Internet Use (Key stage 2)

We use the school computers and the Internet connection for learning. These rules will help us to be fair to others and to keep everyone safe.

- I will ask permission before entering any website, unless my teacher has already approved that site and never go on the Internet when an adult is not present.
- I will not go into other people's files
- I will not bring software into school without permission
- I will only email people I know, or who have been approved by my teacher.
- The messages I send will be polite and responsible
- When sending email I will only use my first name and the school address – never my full name, home address or telephone number.
- I will ask permission before opening an email or an email attachment sent by someone I do not know.
- I will not 'chat' on the Internet
- If I see anything I am unhappy with or I receive messages I do not like I will tell a teacher immediately.
- I know that the school may check my computer files and may monitor the Internet sites that I visit.
- I understand that if I deliberately break the rules I could be stopped from using the Internet or school computers.

The school may exercise the right by electronic means to monitor the use of the school's computer systems, including the monitoring of websites, the interception of email and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is, or may be, taking place, or the system is, or maybe, being used for criminal purposes or for the storing of text or imagery which is unauthorised or unlawful.

Year 3:.....

Date:.....

Year 4:.....

Date:.....

Year 5:.....

Date:.....

Year 6:.....

Date:.....

Reviewed by Teaching & Learning Committee – Summer 19
Review due: Summer 20