Cockfield Primary School

Online Safety Policy

Document Control

Updated:	
Person responsible:	Headteacher
Written by:	
Monitored by:	Headteacher
Reviewed by:	
Next review:	
Adopted on:	
Signed:	

1. INTRODUCTION

Computing 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, Cockfield Primary School has built in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Computing covers a wide range of resources including web-based, games consoles (eg Wii, Xbox, Playstation), PCs, camcorders, digital cameras and portable laptops. It is also important to recognise the constant and fast-paced evolution of computing within our society as a whole.

Currently the internet technologies children are using inside the classroom include:

- Interactive learning websites
- Smart screens
- Digital cameras
- Video equipment
- E-mail
- I-pads
- Laptops

The internet technologies some children are using at home can include:

- Websites
- Game stations
- Digital video equipment
- e-mail
- Instant Messaging and Skype
- Chat Rooms and Social Networking
- Blogs and Wikis
- Pod casting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much computing, 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.

At Cockfield Primary School, we understand the responsibility to educate our pupils on on-line safety 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.

Both this policy and the attached *Acceptable Use Agreement* (for all staff, governors, visitors and pupils) are inclusive of both internet technologies provided by the school (such as PCs, laptops, interactive whiteboards, digital cameras, video equipment, etc) and technologies owned by staff but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs, portable media players, etc).

Children are not permitted to bring in a mobile phone without prior permission from the Headteacher. If a child brings in a data storage device (memory stick, CD, etc) it must not be plugged into the school network **unless the school has virus scanned it first**.

2. ROLES AND RESPONSIBILITIES

As on-line safety is an important aspect of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The named on-line safety curriculum lead in our school is Mrs L Sturgeon. All members of the school community have been made aware of who holds this post.

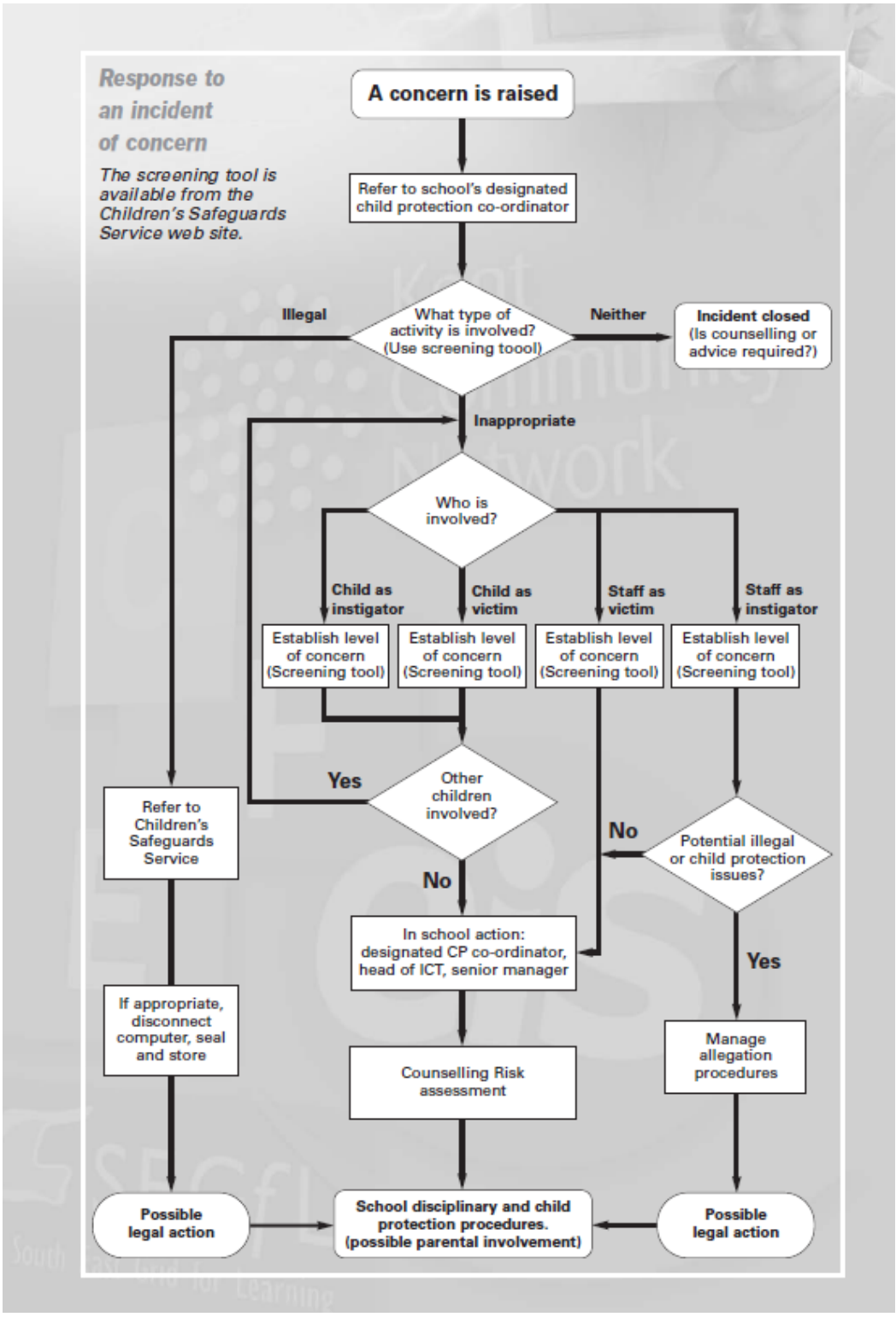
It is the role of the on-line safety co-ordinator to keep abreast of current issues and guidance through organisations such as Suffolk LA, CEOP (Child Exploitation and Online Protection) and Childnet.
It is the responsibility of all staff to report any online safety issues or reports of cyberbullying to Mrs Sturgeon. This will then be logged on the online safety incident log (see appendix 3) and any safeguarding issues or breaches of school policies will be dealt with higher by headteacher Mrs Harkin.

The Senior Leadership Team and Governors are updated by the on-line safety curriculum lead and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's *Acceptable Use Agreements* for staff, governors, visitors and pupils (see appendices), is to protect the interests and safety of the whole school community. It is also linked to the Safeguarding and Anti-Bullying policies.

3. ON-LINE SAFETY SKILLS DEVELOPMENT FOR STAFF

Our staff receive information and training for on-line safety issues in the form of updates at staff meetings by the co-ordinator. New staff receive information on the school's *Acceptable Use Agreement* as part of their induction. A member of our staff has completed CEOP on-line safety training. All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online -Safety and know what to do in the event of misuse of technology by any member of the school community:



4. ON-LINE SAFETY IN THE CURRICULUM

Computing and online resources are increasingly used across the curriculum. We believe it is essential for on-line safety guidance to be given to the pupils on a regular and meaningful basis. On-line safety is embedded within our curriculum and we continually look for new opportunities to promote on-line safety. The school has a framework for teaching internet skills in Computing/ PSHE lessons. The school provides opportunities within a range of curriculum areas to teach about on-line safety and staff use posters to remind children of how to be safe online whenever the internet is being used. There are also two children from each class that are e-cadets that have received training in supporting their

friends to be safe online. They play an active role in reminding everyone how to be safe online each lesson when the internet is being used.

Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the on-line safety curriculum. Pupils are made aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.

Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities. Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies, i.e.

parent/carer when at home

teacher/trusted staff member at school, or

an organisation such as Childline/CEOP report abuse button at both home and school

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

The school will provide supervised access to internet resources (where reasonable) through the school's network. Staff will preview any recommended sites before use. Raw image searches are discouraged when working with pupils. If internet research is set for homework, specific sites must 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.

5. PASSWORD SECURITY

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 and are changed when prompted. Staff do not leave a workstation having access to personal data unattended without locking the workstation or logging off from the network/machine.

6. DATA SECURITY

The accessing and appropriate use of school data is something that the school takes very seriously. Staff are aware of their responsibility when accessing school data. Level of access to school data is determined by the Headteacher.

- Staff do not send emails or attachments that contain personal data unless the personal data is encrypted and any passwords or keys are sent using a different medium.
- Any printouts of personal and sensitive data must be kept securely and disposed of appropriately when no longer required.
- Personal data is not stored on mobile storage devices (USB storage devices, CDs, DVDs, data keys, etc) unless it is encrypted.

- Bulk transfer of personal data is only sent to third parties using secure protocols.
- Administration and financial databases are backed up nightly externally by Gipping- the school technology support company.
- Wireless networks have WPA encryption as a minimum.
- Third party suppliers are only granted access to the school computing system after they have signed a Confidentiality Agreement. ie Gipping
- The school data protection registration is up to date and renewed annually.
- The school annually carries out a safety audit using the: on-line safety Audit Tool Laptops and other computing equipment are not left in unattended vehicles.

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

7. INFRASTRUCTURE

Cockfield Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account: *Data Protection Act 1998*, *The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*, *Regulation of Investigatory Powers Act 2000*,*Human Rights Act 1998*.
The school will work with E2BN the Internet Service Provider to ensure that systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL must be reported to the online safety Coordinator and recorded.
This task requires both educational and technical experience. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Staff and pupils are aware that school based e-mail and internet activity can be monitored and explored further if required. The school does not allow pupils access to internet logs.

If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the on-line safety co-ordinator, who will record the details of the incident and report it to the external IT company Gipping, so the suspect site can be filtered out.

If pupils wish to bring in work on removable media it must be given to the teacher for a virus check first.

8. MANAGING SOCIAL NETWORKING SITES, BLOGS, WIKIS

Staff may only create blogs or wiki spaces in order to communicate with pupils. If used responsibly both outside and within an educational context these can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites. Once these sites have been created for educational purposes the password should be changed so that

children cannot continue to work on them at home as they are no longer checked by a member of staff and could potentially be used inappropriately.

At present, the school endeavours to deny access to social networking sites to pupils within school:

- Pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to never place images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/home phone numbers, school details, IM/ e-mail address, specific hobbies/ interests).
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.

Our pupils are asked to report any incidents of cyber-bullying to the school.

9. PERSONAL MOBILE DEVICES

The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device. The school is not responsible for the loss, damage or theft of any personal mobile device. The sending of inappropriate text messages between any members of the school community is not allowed.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device. Parents are reminded that any images taken during school events must never be shared on social media.

Children are permitted to bring mobile phones into school, particularly older children travelling home independently after school, however they must be handed in to the school office where they are locked away until the end of the school day.

10. MANAGING E-MAIL

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail cannot be considered private.

Educationally, e-mail can offer significant benefits including: direct written contact between schools on different projects, be they staff based or pupil based, within school or international.

We recognise that pupils need to understand how to style an e-mail in relation to their age and good "netiquette".

The school gives all staff their own e-mail account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. This should be the account that is used for all school business.

Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.

E-mail sent to an external organisation must be written carefully before sending, in exactly the same way as a letter written on school headed paper. Staff sending e-mails to external organisations, parents or pupils are strongly advised to cc. the Headteacher.

Pupils may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes. All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to:

- the use of appropriate language
- not revealing any personal details about themselves or others in e-mail communication
- not arranging to meet anyone without specific permission.

Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail.

Staff must inform the on-line safety co-ordinator if they receive an offensive e-mail.

11. 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. With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils. Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of others. This includes when on field trips.

12. PUBLISHING PUPIL'S IMAGES

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, e.g. an exhibition promoting the school
- general media appearances, e.g. local/national media/press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting children's work on the internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Images/films of children are stored on the school's network.

13. MISUSE AND INFRINGEMENTS

Complaints

Complaints relating to on-line safety should be made to the on-line safety co-ordinator/Headteacher. Incidents should be logged and the *Flowcharts for Managing an on-line safety Incident* should be followed (see section 3).

Inappropriate material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the on-line safety co-ordinator. Deliberate access to inappropriate materials by any user will lead to:

- the incident being logged by the on-line safety co-ordinator
- depending on the seriousness of the offence, investigation by the Headteacher/LA
- immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (See flowchart.)

Users are made aware of sanctions relating to misuse or misconduct. All staff are aware of the policy and the children have signed an *Acceptable Use Agreement*.

14. EQUAL OPPORTUNITIES

Pupil with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the school's on-line safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of on-line safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of on-line safety. Internet activities are planned and well managed for these children.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting on-line safety both in and outside of school. We regularly consult and discuss on-line safety with parents/carers and seek to promote a wide understanding of the benefits related to IT and associated risks.

Parents/carers are asked to read through and sign *Acceptable Use Agreements* on behalf of their child on admission to school. Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g. on the school website).

The school disseminates information to parents relating to on-line safety where appropriate in the form of:

- Information and celebration evenings
- Posters
- Website
- Newsletter items
- Learning together workshops

15. CURRENT LEGISLATION

Acts relating to monitoring of staff e-mail

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts relating to on-line safety

Racial and Religious Hatred Act 2006

It is a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a

position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

Communications Act 2003 (section 127)

Sending by means of the internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1- 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

access to computer files or software without permission (for example using another person's password to access files)

unauthorised access, as above, in order to commit a further criminal act (such as fraud) impair the operation of a computer or program UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 - 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone

under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997: A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Education and Inspections Act 2006

An Act to make provision about primary, secondary and further education and about training; to make provision about food or drink provided on school premises or in connection with the provision of education or child care; to provide for the establishment of an Office for Standards in Education, Children's Services and Skills and the appointment of Her Majesty's Chief Inspector of Education, Children's Services and Skills and make provision about the functions of that Office and that Chief Inspector; to provide for the amendment of references to local education authorities and children's services authorities; to amend section 29 of the Leasehold Reform Act 1967 in relation to university bodies; and for connected purposes.

Cockfield Primary School endorses the advice in the sites listed below and expects parents and children to read and abide by the guidance therein.

16. ON-LINE SAFETY GUIDANCE

Be smart on the internet - Child's Guide to '5 SMART Rules' Leaflet Download: *http://www.childnet-int.org/* is the home website.

http://www.safekids.com/safety-advice-tools

https://www.thinkuknow.co.uk

http://www.getsafeonline.org

17. APPENDIX 1 - ACCEPTABLE USE AGREEMENT: STAFF, GOVERNORS AND VISITORS

18. APPENDIX 2- PRIMARY PUPIL ACCEPTABLE USE

19. APPENDIX 3- ONLINE SAFETY INCIDENT LOG

APPENDIX 1

Acceptable Use of IT and Mobile Phones Policy
Cockfield CEVC Primary School

1. PURPOSE
The policy defines and describes the acceptable use of IT (Information Technology) and mobile phones for school-based employees. Its purpose is to minimise the risk to pupils of inappropriate contact from staff, to protect employees and schools from litigation and to minimise the risk to IT systems.

2. SCOPE
2.1 This policy deals with the use of IT facilities in Cockfield CEVC Primary School and applies to all school-based employees and other authorised users, e.g. volunteers.
2.2. Non school-based staff is subject to the County Council's IT Acceptable Use Policy.

3. SCHOOL RESPONSIBILITIES
3.1 The Governing Body is responsible for ensuring that its employees act in a lawful manner, making appropriate use of school technologies for approved purposes only.
3.2 The Governing Body is responsible for adopting relevant policies and the Head teacher for ensuring that staff are aware of their contents.
3.3 The Bursar is responsible for maintaining an inventory of IT equipment and a list of school laptops/IPADS and cameras and to whom they have been issued.
3.4 If the Head teacher has reason to believe that any IT equipment has been misused, he/she should consult the LADO at Suffolk County Council without delay. The Area Personnel Officer will agree with the Head teacher and CSD's Policy and Compliance Manager an appropriate strategy for the investigation of the allegations. Incidents will be investigated in a timely manner in accordance with agreed procedures.
3.5 Head teachers should make it clear that internal school staff should not carry out any investigations unless they are both qualified and authorised to do so.
3.6 The Head teacher is responsible for removing staff, governors and pupils from the website when they leave the school. Passwords must be changed where necessary.

4 USER RESPONSIBILITIES
4.1 Staff found to be in breach of this policy may be disciplined in accordance with the disciplinary procedure. In certain circumstances, breach of this policy may be considered gross misconduct resulting in termination of employment. Users must report all suspected breaches of this policy to the Head teacher.
4.2 Users and their managers are responsible for ensuring that adequate induction, training and support is undertaken to implement this policy.
4.3 By logging on to IT systems, users agree to abide by this Acceptable Use policy and other policies that relate to the use of IT.

4.4 All users are expected to act in a responsible, ethical and lawful manner with the understanding that school electronic and manual information may be accessible to the public under the Freedom of Information Act 2000. Users should uphold privacy and confidentiality in accordance with the Data Protection Act 1998. Care must also be taken not to breach another person's copyright, trademark or design, nor to publish any defamatory content.
4.5 Staff who have been given the use of a school laptop will be expected to sign for its use on receipt. Staff may use school equipment for authorised business use only, except as allowed for in paragraph 5.1.
4.6 Staff must follow authorised procedures when relocating IT equipment or taking mobile devices offsite.
4.7 No one may use IT resources in violation of license agreements, copyrights, contracts or national laws, or the Standing Orders, policies, rules or regulations of the school or the County Council.
4.8 Users are required to protect their password and not share their account details with others for their use, nor utilise another users' account or misrepresent their identity for any reason. Users must not under any circumstances reveal their password to anyone else.
4.9 No user shall access (e.g., read, write, modify, delete, copy, move) another user's personal electronic documents (including email) without the owner's permission or as allowed by this policy or by law.
4.10 Users must not load or download software on any device without the authorisation of the Head teacher. Periodic audits of software held on IT equipment will be undertaken.
4.11 Users must take care to store sensitive information, e.g. pupil data safely and to keep it password protected, on all school systems, including laptops.
4.12 Network connected devices must have school approved anti-virus software installed and activated. Users may not turn off anti-virus software. All users of IT resources have the responsibility to take precautions to prevent the initial occurrence and subsequent spreading of a computer virus. No one may knowingly create, install, run, or distribute any malicious code (e.g. viruses, Trojans, worms) or another destructive program on any IT resource.
4.13 No one may knowingly or willingly interfere with the security mechanisms or integrity of IT resources. No one may use IT resources to attempt unauthorised use, or interfere with the legitimate use by authorised users, of other computers on internal or external networks. Access to networks will be monitored.
4.14 Within the terms of the Data Protection Act 1998, Human Rights Act 1998 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the County Council or school may record or inspect any information transmitted through or stored in its computers, including e-mail communications and individual login sessions, without notice when:

- There is reasonable cause to believe the user has violated or is violating this policy, any guidelines or procedures established to implement this policy.
- An account appears to be engaged in unusual or unusually excessive activity.
- It is necessary to do so to protect the integrity, security, or functionality of IT resources or to protect the County Council or its partners from liability.
- Establishing the existence of facts relevant to the business.
- Ascertaining or demonstrating standards which ought to be achieved by those using the IT facilities
- Preventing or detecting crime

- Investigating or detecting unauthorised use of IT facilities
- Ensuring effective operation of IT facilities
- Determining if communications are relevant to the business (for example, in the last resort where an employee is off sick or on holiday and business continuity is threatened)
- It is otherwise permitted or required by law.

4.15.1 Do not send private, sensitive or confidential information by unencrypted email – particularly to an external recipient - if accidental disclosure could lead to significant harm or embarrassment, anonymise personal data where possible e.g. by using initials. Use passwords on sensitive documents that must be sent to external recipients.
4.15.2 Websites should not be created on school equipment without the written permission of the Head teacher.
4.15.3 No one may use IT resources to transmit abusive, threatening, or harassing material, chain letters, spam, or communications prohibited by law. No one may abuse the policies of any newsgroups, mailing lists, and other public forums through which they participate from a school account.
4.15.4 The following content should not be created or accessed on IT equipment at any time:

- Pornography and “top-shelf” adult content
- Material that gratuitously displays images of violence, injury or death
- Material that is likely to lead to the harassment of others
- Material that promotes intolerance and discrimination on grounds of race, sex, disability, sexual orientation, religion or age
- Material relating to criminal activity, for example buying and selling illegal drugs
- Material relating to any other unlawful activity e.g. breach of copyright
- Material that may generate security risks and encourage computer misuse

4.16 It is possible to access or be directed to unacceptable Internet sites by accident. These can be embarrassing and such sites can be difficult to get out of. If staff have accessed unacceptable content or are in receipt of unacceptable material via email, they should inform the Head teacher. This may avoid problems later should monitoring systems be alerted to the content.

5 PERSONAL USE & PRIVACY

5.1 In the course of normal operations, IT resources are to be used for business purposes only. The school permits limited personal use of IT facilities by authorised users subject to the following limitations:

- Personal use must be in the user’s own time and must not impact upon work efficiency or costs.
- The level of use must be reasonable and not detrimental to the main purpose for which the facilities are provided.
- Personal use must not be of a commercial or profit-making nature.
- Personal use must not be of a nature that competes with the business of the school or conflicts with an employee’s obligations.

5.2 Personal use of the Internet must not involve attempting to access the categories of content described in section 4.18 that is normally automatically blocked by web filtering software.

5.3 Staff are advised not to give their home telephone number or their mobile phone number to pupils.
5.4 Photographs and videos of pupils should not be taken with mobile phones.
5.5 Staff are advised not to make use of pupils' mobile phone numbers either to make or receive phone calls or to send to or receive from pupil's text messages.
5.6 Staff should not enter into instant messaging communications with pupils
5.7 Staff may not use their mobile phones while supervising the pupils, unless an emergency concerning a/the pupils has arisen.

6. DIGITAL CAMERAS
6.1 Personal cameras or cameras on mobile phones are not to be used in school unless permission has been granted by the Head teacher.
6.2 Personal photographs are not to be downloaded onto school equipment
6.3 Students may not take photographs without the permission of the Head teacher

Signed _____Headteacher

Signed _____Chair of Governors

Date _____

Review Date March 2019

APPENDIX 2

Cockfield CEVC Primary School

Online Safety & Computing

These rules will help us to be fair to others, to keep everyone safe and look after the equipment.

- When working or using computers in school, I will follow the school behaviour code and have a positive attitude to my work.

- I will treat all people with respect, for example:
  By listening carefully to all adults

  By keeping computer speaker noise levels at a sensible volume

- I treat school and individual property with respect, for example:
  By taking care of all the equipment.

- I do not use the equipment if I am unsure how to use it – if problems arise or I make a mistake in my work, I ask a member of staff for help.

- I work safely and remember that – I never touch electrical equipment without permission

- When I have finished using a computer I make sure I log off and at the end of the day shut down.

- I will ask permission before entering any website, unless my teacher has told me to look at one.

- If I work on a network, I will use only my own password.

- I will only e-mail people my teacher has told me to.

- The messages I send will be polite and sensible.

- I will ask for permission before opening e-mail.

- I know that the school may check my computer files or the Internet sites I visit.

- I understand that if I deliberately break these rules, I could be stopped from using the internet or computers.

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web sites, the interception of e-mail and deletion of inappropriate materials.

Consent Form

Cockfield CEVC Primary School Online Safety Please complete, sign and return to the school office	
Pupil:	Class:
Pupil's Agreement I have read and understand the school rules or have had the rules explained to me for Online Safety. I will use the computer system and internet in a responsible way and obey these rules at all times.	
Signed:	Date:
Parent's Consent for Internet Access I have read and understood the school rules for responsible IT use and give permission for my son / daughter to access the internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. *I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.*	
Signed:	Date:
Please print name:	
Parent's Consent for possible future Web Publication of Work and Photographs I agree that, if selected, my son / daughter's work may be published on the school Web site. I also agree that photographs that include my son / daughter may be published subject to the school rules that photographs will not clearly identify individuals and that names will not be used.	
Signed:	Date:

APPENDIX 3

Cockfield Primary School Online Safety Incident Log

Date	Person filling out form	Location incident took place	Incident detail	Incident response	Outcome of Investigation.