Think Believe Achieve

Sexton's Manor Community Primary School Online Safety and Acceptable Use Policy

INTRODUCTION

Since the introduction of IT, education has seen a dramatic change in the way we teach and learn and it is now seen as an essential resource to support learning. IT is increasingly becoming an important part of our lives that we often depend on computers to complete daily tasks. Therefore, Sexton's Manor School realises the need to educate its pupils and staff on how to use IT equipment responsibly, in order to provide lifelong learning skills for education and employment.

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. It also outlines procedures and sanctions for the inappropriate use of IT equipment.

1 SCOPE

1.1 This policy deals with the use of IT facilities in Sexton's Manor School and applies to all school-based employees and other authorised users. Any adult making regular visits to the school needs to be aware of the 'Important Online Safety Information for Visitors' (kept in the signing in book in the reception area -see Appendix 3) and must sign to notify they have read and understood them.

1.2. Non-school based staff are subject to the County Council's IT Acceptable Use Policy.

2 SCHOOL RESPONSIBILITIES

2.1 The headteacher and Governing Body is responsible for ensuring that its employees act in a lawful manner, making appropriate use of school technologies for approved purposes only.

2.2 The Governing Body is responsible for adopting relevant policies and the headteacher for ensuring that staff are aware of their contents.

2.3 The School Office is responsible for maintaining an inventory of IT equipment and a list of school laptops and mobile phones and to whom they have been issued.

2.4 Mrs D. Knight is the senior designated person for safeguarding. The online safety lead is Mrs. J. Jones and the governor is Mrs G. Brockwell. Any misuse or incidents must be reported at once to Mrs D. Knight and / or Mrs J. Jones.

2.5 If the headteacher has reason to believe that any IT equipment has been misused, she will follow, in conjunction with the online safety lead, the referral pathway set out in Appendix 1a. Advice will be sought depending on the severity or the nature of the incident. All incidents pertaining to online safety, however small, will be recorded in school using the 'Online safety incident referral form', Appendix 1b. This form makes reference to the 'Sentencing Advisory Panel' (SAP) Level as outlined in Appendix 1c to help determine the appropriate response (if required).

2.6 The headteacher should make it clear that internal school staff should not carry out any investigations unless they are both qualified and authorised to do so, ie online safety lead training.

2.7 The headteacher and staff are responsible for promoting online safety across the curriculum. This taught content is set out in Appendix 2.

2.8 The Governors should be made aware of any online safety incidents and any changes to the online safety curriculum.

2.9 The Governors **MUST** ensure online safety is covered within an awareness of safeguarding and how it is being addressed within Sexton's Manor school. It is the responsibility of Governors to ensure that all safeguarding guidance and practices are embedded and appropriate actions are taken.

2.10 An online safety Governor should undertake regular audits and pupil perceptions and challenge the school with appropriate questions - See Appendix 4.

2.11 This policy is displayed on the website. The school website links to various resources for parents and children and a link to www.thinkuknow.com with its 'red button' facility features on the home page.

2.12 The online safety policy and AUP is reviewed annually, with up-to-date information. Training is available for all staff to teach online safety and for parents to feel informed and know where to go for advice.

2.13 Filtering is set to the correct level for staff and children for all IT equipment and the technician is informed and carries out work according to current guidelines.

2.14 All adults are aware of the filtering levels and why they are there to protect children and young people.

3 USER RESPONSIBILITIES

3.1 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 headteacher.

3.2 The headteacher and online safety lead are responsible for ensuring that adequate induction, training and support is undertaken to implement this policy.

3.3 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.

3.4 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 and personal use see 4.1. Staff must follow authorised procedures when relocating IT equipment or taking mobile devices offsite. Laptops must be kept out of sight, for example in the boot of a car and they must be logged out of when not being used. Food and drink should be kept away from laptops. If taking a laptop off-site it must be signed out.

3.5 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.

3.6 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. ('Guest' and 'student' user account have been set up which allow internet access but no access to the staff area on the school network?)

3.7 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.

3.8 Users must not load or download software on any device without the authorisation of the headteacher. The school's IT technician maintains a list of software held on IT equipment and all licensing.

3.9 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.

3.10 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.

3.11 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.

3.12 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.

3.13 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. Ensure that the tone of emails is in keeping with all other methods of communication.

3.14 Websites should not be created on school equipment without the written permission of the Headteacher.

3.15 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.

3.16 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

3.17 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 headteacher / online safety lead. This may avoid problems later should monitoring systems be alerted to the content. The headteacher will then respond using the protocol set out in Appendix 1a (if required). Staff should undertake pre-lesson online checks to ensure that content being accessed online is suitable for children (using a children's laptop in school).

3.18 It is requested that accessing social networking sites is only permitted in personal time and on user's own IT equipment in school and that social networking profiles are set to private, helping to block unwanted communications. Staff are not to add pupils as 'friends' on social networking sites and it is recommended that this applies to adding parents of children as 'friends'. Staff should not have pupil images displayed on social networking sites. Staff must not refer to children or incidents that have taken place at school. Staff must ensure that their online presence is responsible and the reputation of the school is maintained.

3.19 Staff update pages on the school website and these are subsequently authorised by the headteacher or online safety lead. Parents give consent for images of their child to be displayed on the school's website or local press when admitted to the school and there are opportunities to update this regularly. Pupils full names will not be used on the website nor given to the press.

3.20 The contact details on the website should be the school address, e-mail and telephone number. Staff or student's personal details will not be published.

3.21 All printing must be for school related activities. Staff should take every step to ensure confidential printing.

3.22 It is not acceptable for pupils, parents or colleagues to bully each other via social media as it is unacceptable to do so face to face. Staff should never respond or retaliate to cyberbullying incidents. Any incidents should be reported to the headteacher or online safety lead and evidence of the abuse should be saved by taking prints of messages or screen shots and dates and times recorded. A meeting will be set up with the perpetrator who will be asked to remove the abusive material. If the perpetrator refuses to remove the material further reporting can take place e.g. on social networking sites. If the comments are threatening or abusive, sexist or of a sexual nature or constitute a hate crime, the local police can be contacted.

4 PERSONAL USE & PRIVACY

4.1 In the course of normal operations, IT resources are to be used for school 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.

4.2 Personal use of the Internet must not involve attempting to access the categories of content described in section 3.16 that is normally automatically blocked by web filtering software.

4.3 Staff email accounts should remain for their own professional use and any communications between parents and school should be via the school office admin email account.

5 CHILDREN AND YOUNG PEOPLE

5.1 Children and young people should be:

- Involved in the review of 'My online safety agreement' (See Appendix 5) at Sexton's Manor in line with this policy being reviewed and updated.
- Responsible for following the 'My online safety agreement' whilst within Sexton's Manor or whenever a new child attends the school for the first time. School rules for online safety must be displayed in each classroom.
- Taught to use the internet in a safe and responsible manner through computing, PSHE or other clubs and groups.

- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).
- Supervised when using the internet at all times.
- Hand any mobile phones into the School Office for safekeeping during the day.

6 IN THE EVENT OF INAPPROPRIATE USE:

6.1 Parents will be informed if any child is found to be misusing the internet by not following 'My online safety agreement'. The issue of a child or young person deliberately misusing online technologies should be addressed according to the procedural steps in Appendix 1a and recorded on the incident log in Appendix 1b.

6.2 In the event that a child or young person **accidentally** accesses inappropriate materials the child should report this to an adult immediately. Staff should close the lid of the laptop or close the screen and report to the online safety lead or headteacher immediately. If necessary, the image should be reported to CEOP and parents will be informed. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. Thinkuknow and Childline information are displayed in school.

6.3 It is not acceptable for pupils, parents or colleagues to bully each other via social media as it is unacceptable to do so face to face - see point 3.22.

7 MOBILE PHONE COMMUNICATIONS AND INSTANT MESSAGING

7.1 Staff are advised not to give their home telephone number or their mobile phone number to pupils and parents. The school mobile phone must be taken on trips where the potential need for parent helpers to contact a member of staff via a mobile phone forms part of planned emergency procedures.

7.2 Photographs and videos of pupils should absolutely not be taken with mobile phones. Photographs and video should only be taken on school equipment.

7.3 Staff should only communicate electronically with pupils from school accounts on approved school business.

7.4 During the school day, staff may use mobile phones *in their own time* briefly and privately.

7.5 Mobile phones must be kept out of reach of children and out of view.

7.6 Parent helpers/visitors/students must not use their mobile phones whilst helping in the school.

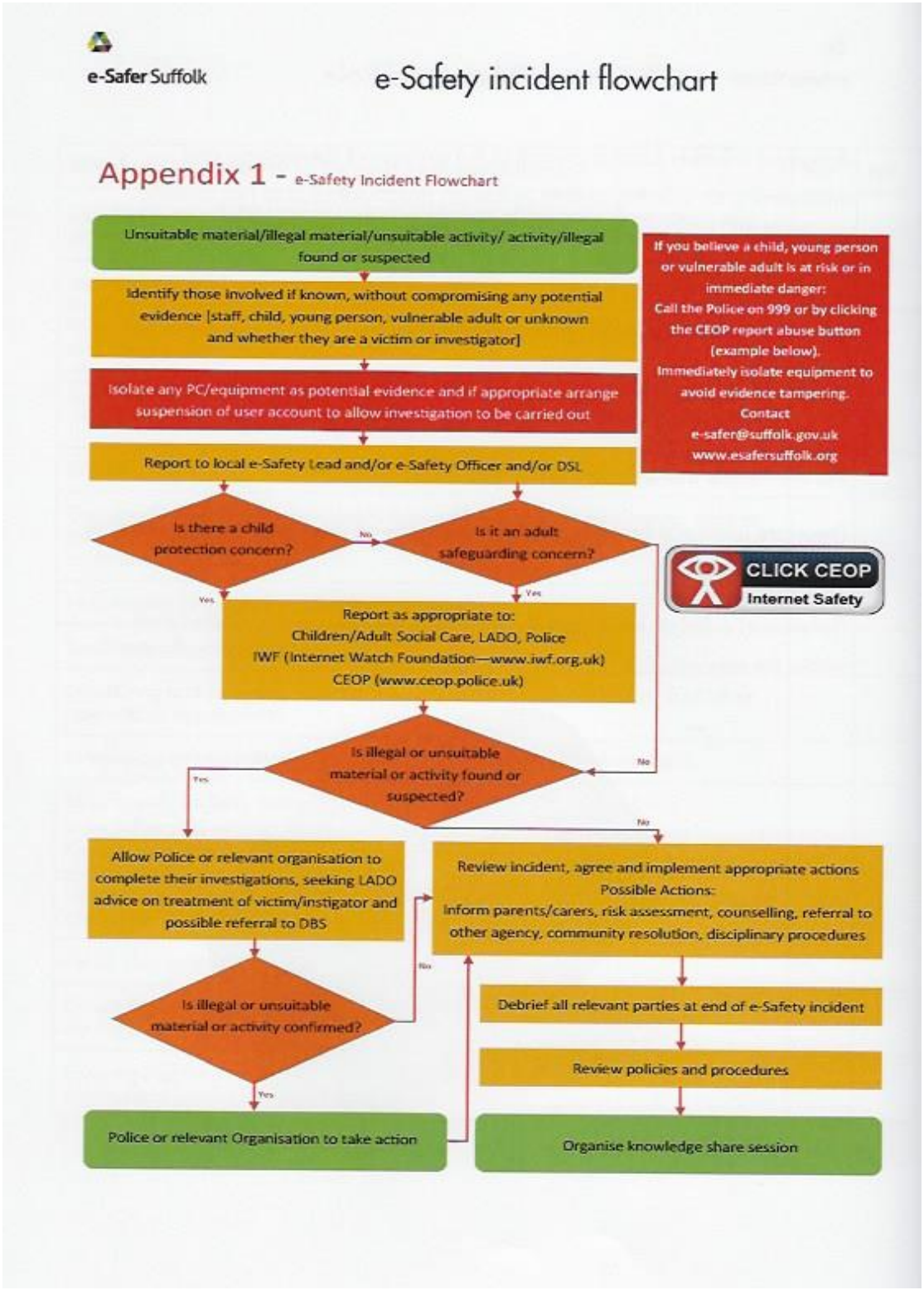
To be reviewed annually.

Adopted at Governing Body meeting on…….

Signed…….

Date: March 2017

Appendix 1a Reporting and Referral of online safety Incidents



1b Online safety incident log

It is essential that all Online Safety incidents are monitored and logged

Date	Contact details (referrer)	Location incident took place (home/ school)	Incident detail including level if necessary (see appendix 1c)	Action taken	Outcome of investigation	Is a child or young person involved?	Is this a safeguarding issue?

Appendix 1c Screening scale of online safety Incidents

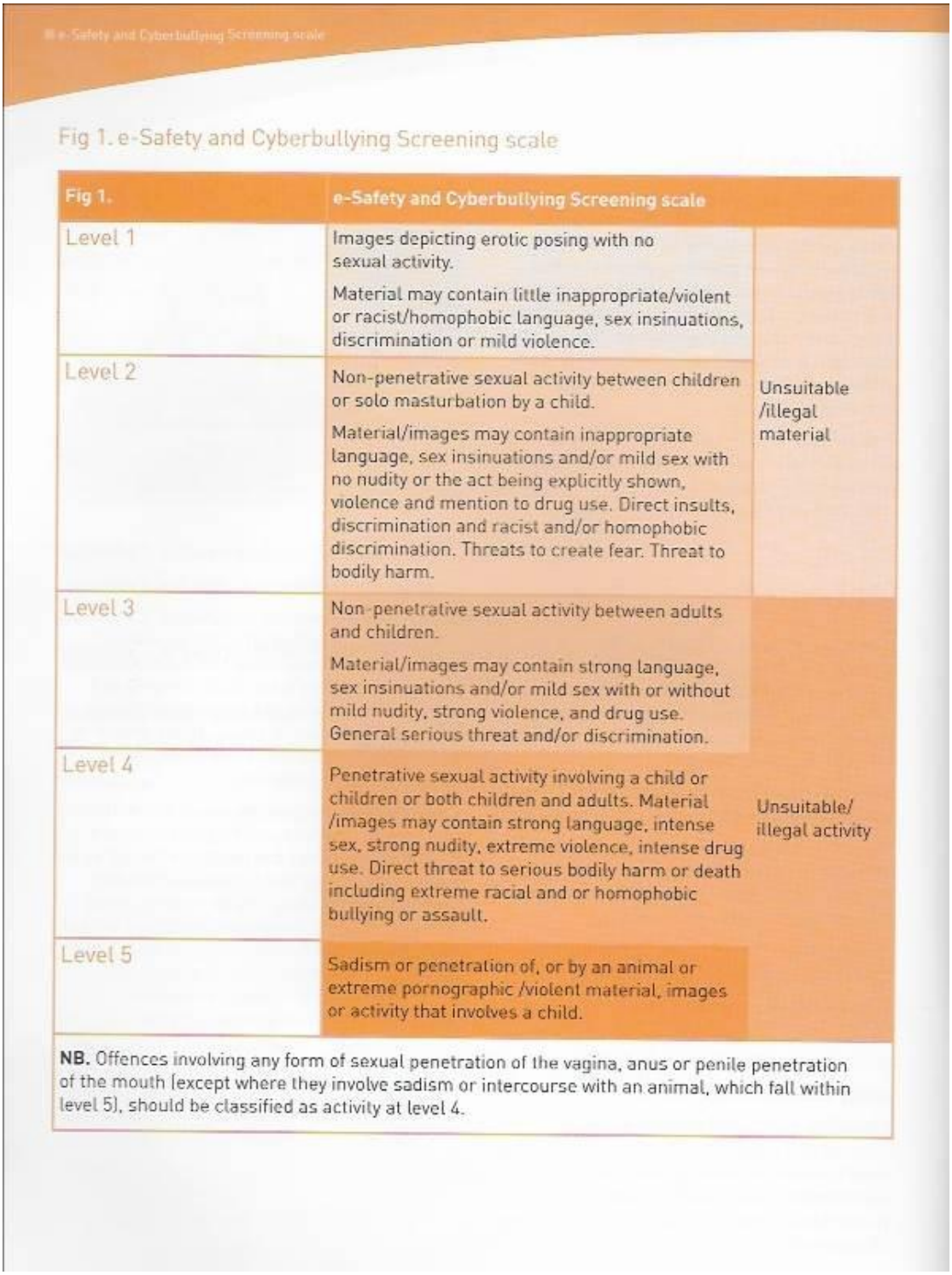


Fig 1. e-Safety and Cyberbullying Screening scale

Fig 1.	e-Safety and Cyberbullying Screening scale	
Level 1	Images depicting erotic posing with no sexual activity. Material may contain little inappropriate/violent or racist/homophobic language, sex insinuations, discrimination or mild violence.	Unsuitable /illegal material
Level 2	Non-penetrative sexual activity between children or solo masturbation by a child. Material/images may contain inappropriate language, sex insinuations and/or mild sex with no nudity or the act being explicitly shown, violence and mention to drug use. Direct insults, discrimination and racist and/or homophobic discrimination. Threats to create fear. Threat to bodily harm.	
Level 3	Non-penetrative sexual activity between adults and children. Material/images may contain strong language, sex insinuations and/or mild sex with or without mild nudity, strong violence, and drug use. General serious threat and/or discrimination.	Unsuitable/ illegal activity
Level 4	Penetrative sexual activity involving a child or children or both children and adults. Material /images may contain strong language, intense sex, strong nudity, extreme violence, intense drug use. Direct threat to serious bodily harm or death including extreme racial and or homophobic bullying or assault.	
Level 5	Sadism or penetration of, or by an animal or extreme pornographic /violent material, images or activity that involves a child.	

NB. Offences involving any form of sexual penetration of the vagina, anus or penile penetration of the mouth (except where they involve sadism or intercourse with an animal, which fall within level 5), should be classified as activity at level 4.

Appendix 2 National Curriculum online safety Content

Pupils at Sexton's Manor are taught at Key Stage 1 to:

- use technology purposefully to create, organise, store, manipulate and retrieve digital content
- recognise common uses of information technology beyond school
- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils at Sexton's Manor are taught at Key Stage 2 to:

- understand computer networks including the internet; how they can provide multiple services, such as the world wide web; and the opportunities they offer for communication and collaboration
- use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
- select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information
- use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

Appendix 3

Important Online Safety Information for Visitors

Sexton's Manor Community Primary School is committed to educating children and adults in online safety.

Please sign to show you have read and understood the following information.

- Sexton's Manor has an online safety policy which outlines what we believe to be acceptable use of school technologies.

- If you are planning to use IT within the school, describe to a member of the office staff your planned activity and they will advise you as to whether you will need to read the full policy.

- If you are asked to help children with IT in school, please read the 'My Online Safety Agreement' for the pupils. In the event of any unsuitable material being accidently accessed, please close the lid on the laptop and notify the class teacher.

- All users of IT in the school are expected to behave in a responsible, lawful and ethical manner.

- Be aware that our school network is filtered to keep our children safe and usage can be monitored.

- No mobile or smartphones should be used whilst helping in school and should be set to silent, vibrate or turned off.

- No photographs or video must be taken of the children, staff or premises without the express permission of the headteacher.

Thank you for your support.

Appendix 4 A focus for monitoring

A good school should expect positive, transparent answers to all of the following questions. Both the online safety lead and the online safety governor use these questions as a prompt to:
a) hold the online safety lead accountable.
b) elicit the knowledge and understanding of children in terms of online safety.

Sample questions for School Leadership including the Governing Body:

1 How do you ensure that all staff receive appropriate online safety training that is relevant and regularly up to date?
2 What mechanisms does the school have in place to support pupils and staff facing online safety issues?
3 How does the school educate and support parents and whole school community with online safety?
4 Does the school have online safety policies and acceptable use policies in place? How does the school know that they are clear and understood and respected by all?
5 Describe how your school educates children and young people to build knowledge, skills and capability when it comes to online safety. How do you assess its effectiveness?

Sample questions for pupils:

1 If you felt uncomfortable about anything you saw, or if anybody asked you for your personal details such as your address on the internet would you know where to go for help?
2 If anybody sent you hurtful messages on the internet or on your mobile phone would you know who to tell?
3 Can you tell me one of the rules your school has for using the internet?

Sample questions for staff:

1 Have you had any training that shows the risks to your and pupils online safety?
2 Are there policies in place that clearly demonstrate good and safe internet practice for staff and pupils?
3 Are there sanctions in place to enforce the above policies?
4 Do all staff understand what is meant by the term cyber-bullying and the effect it can have on themselves and pupils?
5 Are there clear reporting mechanisms with a set of actions in place for staff or pupils who feel they are being bullied online?
6 Does the school have any plans for an event on Safer Internet Day?

Appendix 5

My Online Safety Agreement

This is our class agreement for using IT and the internet safely and responsibly at Sexton's Manor. I know that I must follow these guidelines closely or there may be consequences, like telling my parents or missing out on some IT lessons.

- **I will use IT and the internet safely and responsibly to help me learn and to look after myself and others.**
- **I will only send polite and friendly messages and emails to people I know or who my teacher has approved.**
- **I will never go online in school without telling an adult first.**
- **I will never give out my passwords or personal information, like my name, school, address, email or phone number.**
- **I will never post anything online in school without my teacher's permission.**
- **I will tell an adult if I see anything online that makes me feel uncomfortable.**
- **I will tell an adult if I am contacted online by people I don't know.**

If I need help or feel I can't speak to an adult I know, I can visit www.thinkuknow.co.uk or contact Childline on 0800 11 11.