worcestershire countycouncil

Catshill Middle School and

Catshill First School & Nursery

Online Safety Guidance

Including Acceptable Use Agreements and

Protocols for the Internet

Reviewed: February 2022

Next Review: September 2024

Signature…….. Chair of Committee

Date ……

The school policy for Online Safety, including Acceptable Use Agreements and Protocols for the use of the internet reflects the consensus of opinion of the whole teaching staff and has the full agreement of the Governing Body.

1. Aims

- to ensure that pupils are provided with as safe and secure learning technologies and internet environment as is possible,
- to educate pupils and adults to be aware of, and respond responsibly, to any risks,
- to encourage and support parents, staff and other stakeholders in protecting and educating pupils on how to stay safe online and in the wider world.

2. Roles and responsibilities

Online safety is a whole-school responsibility dependent on all stakeholders eg staff, governors, advisers, parents and, where appropriate, pupils themselves taking responsibility for the use of the Internet and other forms of communication. Of major importance in creating a safe e-learning environment is the internet safety education which occurs in the classroom itself, initiated by the teacher or teaching assistant. Pupils are taught safe and responsible behaviours and are enabled to develop the critical thinking skills to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Whilst the Executive Head Teacher has overall responsibility for safeguarding, which includes online safety issues, a senior leader has delegated responsibility as the online safety Coordinator responsible for online safety management. This is the Head of School.

All members of the school community have core responsibilities within and outside the school environment to:

- use technology responsibly
- accept responsibility for their use of technology
- model best practice when using technology
- report any untoward incidents to the Head Of School using the school procedures
- understand that network activity and online communications are monitored, including any personal and private communications made via the school networks.

3. E-learning technologies

The school subscribes to the accredited County Council Broadband service as its ISP (Internet Service Provider) which provides an effective and safe online learning environment including Internet access, e-mail service and school website hosting. Any new technologies will only be made accessible to the school community when they have been assessed for their nature, content, educational benefit, safety and security. The school maintains a comprehensive inventory of all its ICT equipment including a record of safe and secure disposal.

3.1 Network security and monitoring

The school reviews both physical and network security regularly and monitors who has access to the system:

- Anti-virus software is installed on all computers and updated regularly.
- Central filtering is provided and managed by Smoothwall RADAR. All staff are made aware that if an inappropriate site is discovered it must be reported to the Head of School who will report it to the Network Manager to be blocked. Pupils are taught to tell an adult immediately if they open a site which has unpleasant content or which worries them. All incidents will be recorded in the online safety log for audit purposes.
- Requests for changes to the filtering will be directed to the Head of School in the first instance who will forward these on to the Network Manager or liaise with the Executive

Headteacher as appropriate.

- The school uses Smoothwall RADAR on all school owned equipment to ensure compliance with the Acceptable Use Policies. This is monitored by the Head of School, in liaison with the Network Manager.
- Screen captures are used to follow up inappropriate content, words or images.

3.2 Passwords

- All staff are issued with their own username and password for network access. Any visitors / Supply staff are issued with temporary IDs.
- All pupils have personal logins which they are taught not to share; however it is acknowledged that when pupils work together on a computer one or the other will need to login.
- Teachers have access to SIMS. This service is used for electronic registration. Passwords for servers are cryptic to ensure they are secure. These passwords are available to the School Business Manager and to the Executive Headteacher in case of emergency.

3.3 Mobile technologies

- Chromebooks are provided for teachers for educational purposes and their own professional development. These can be used outside of school, although staff are advised to ensure these are kept safe and secure at all times e.g. they should not be left locked in the boot of a car. The online safety policy and user agreements also apply to such devices at all times.

4. Online Safety Awareness and training

Online safety awareness and education is an essential part of the school' online safety provision.

To achieve this the school:

- provides a programme of online safety learning as part of Computing/PSHE, and reinforces key online safety messages throughout the school curriculum
- makes this policy, and related documents, available on the school website for everyone to access
- updates and reviews this policy, and related documents
- displays relevant online safety information
- provides online safety information to a wide range of stakeholders, and visitors eg. through school newsletters, mailshots, twitter, facebook and workshops
- learning technologies are reviewed by relevant coordinators and their purpose, online safety considerations and ideas for their use are disseminated through curriculum meetings/staff meetings/training sessions
- parents are provided with online safety advice and guidance on the school website, and when appropriate via newsletters or parents' meetings/workshops.

5. Acceptable Use of the Internet

The Internet can provide pupils and all stakeholders with opportunities to experience and use a wide range of activities, resources, and information to support and enhance the learning and teaching across the whole school curriculum. All pupils will be expected to access the Internet unless parents have indicated otherwise at the time their child is admitted to school.

Adults in school who will use e-technologies are asked to read, sign and comply with the relevant online safety/Acceptable Use Agreement.

Parents are asked to discuss with their children the online safety/Acceptable Use Agreement for pupils appropriate to the key stage their child is in, and sign the agreement. The signed online safety agreements will be kept in the school.

Pupils will be taught how to use the internet safely and responsibly as an integral part of online learning across the curriculum and supported by the school's online safety programme. In the spirit of Every Child Matters pupils will be taught how to be safe while online at home as well as at school. Consideration of Keeping Children Safe in Education September 2021, Annex D.

Videos from 'You tube' which are to be used to support and enhance learning and teaching are vetted prior to use with children. Such videos are NOT to be accessed or loaded whilst children are present so must be loaded on full screen prior to children coming into the classroom/hall. Alternatively, when possible the YouTube downloader should be used, depending on the settings of a video itself working within this.

6. Email and Google Suite

The Internet as a means to contact people and organisations is an extremely valuable tool, encouraging the development of communication skills and transforming the learning process by opening up extra possibilities. However, just as in the real world, children may get involved in inappropriate, antisocial or illegal behaviour while using new technologies eg, cyberbullying, identity theft, and arranging to meet people they have met online. The e-mail system is regularly monitored and should not be considered private communication. The school uses the full functionality of google suite and its encrypted security levels. This allows for remote teaching, document sharing and collaboration. This is monitored using Smoothwall.

6.1 Staff

All staff are given a school e-mail address. Staff are advised that LA advice is to always use school email addresses for emails regarding their professional role and responsibilities. Staff are allowed to access personal e-mail accounts on the school system outside directed time and are advised that any messages sent using the school equipment must be in line with the school's e-mail policy. In addition, they are also advised that these messages will be scanned by the monitoring software.

6.2 Pupils

Whilst children will, at times, use emails as part of their learning across the curriculum, the school does not use chat rooms or instant messaging. Children will however be made aware of the risks involved in all of these and ways of avoiding them, as part of their online safety and digital literacy skills development.

Any inappropriate e-mails must be reported to the Head of School as soon as possible.

If any staff believe that a child has been targeted with e-mail messages by parties with criminal intent, the messages will be retained, the incident recorded, and the Governors and the child's parents informed. Advice will also be taken regarding possible further steps, including investigation using forensic monitoring software.

To provide an email environment for pupils which is as safe and secure as possible the school has adopted the following practice:

- steps are taken to verify the identity of any school or child seeking to establish regular e-mail with this school;
- children are taught not to open or respond to emails from a previously unknown source, but to tell the member of staff present in the room so that appropriate action can be

taken.

- to avoid children revealing their identity within e-mail messages, the child's personal address is never revealed, and information is never given that might reveal the child's whereabouts.

7. Use of other communication and mobile technologies

Staff are advised that they should use their own mobile phones sensibly and MUST NOT use them for calls, text messaging, photographs or social networking during learning and teaching time.

No member of staff should use their own personal cameras in school (including cameras on mobile phones) to take photographs of the children. Any photography should always be done on a school camera, which must not be taken home.

Pupils are not allowed to bring mobile phones into school at Catshill First School and Nursery. Mobile phones are handed in to the Office at Catshill Middle School. The Educations and Inspections Act 2006 grants the Executive Headteacher the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Executive Headteacher will exercise this right at his discretion.

The school internet/e-mail facilities should be used only for educational purposes during teaching and learning time. Staff are advised not to, but if they do choose to use school internet facilities for personal purposes, such as online banking or purchasing of items for personal use, this will be at their own risk.

If staff use social networking sites eg. Facebook, Twitter, NO reference is to be made to Catshill First School and Nursery or Catshill Middle School by name, nor by description of events, comments, people, or feelings towards the school/colleagues.

Staff are advised not to accept parents/carers of pupils in school as friends on social networking sites such as Facebook, and to consider carefully any photos they may post which may link them to Catshill First School and Nursery or Catshill Middle School. Using alternative names rather than your full name is a very good way of ensuring people cannot search for you on social media.

Staff should be mindful of unsolicited emails from people they do not know and use the Spam reporting facility as appropriate.

Infringement of these rules, or inappropriate use will be taken as a serious disciplinary issue.

8. Publishing of Content via digital resources or the internet

It is recognised that staff and children may at some time produce and publish materials on an Internet Web Site associated with the School or the County.

The school has its own website, Twitter and Facebook. Materials produced as part of children's learning may be published on it unless parents have indicated otherwise at the time their child is admitted to school. Pupils' full names will not be published outside the school environment. Should anyone wish to contact the school in response to such materials they are advised to contact the school via the school office by email or telephone.

No materials will be published on the Internet which contain any unacceptable images, language or content.

Infringement of these rules will be taken as a serious disciplinary issue.

Parents are advised that they should not take photographs or videos as some parents do not want their children photographed. Parents may take individual photographs of their own children after a special event or performance.

9. Copyright Issues

It is recognised that all materials on the Internet are copyright, unless copyright is specifically waived. It is the school's policy that the copyright of Internet materials will be respected. Where materials are published on the Internet as part of the teacher's professional duties, copyright will remain with the County Council. Internet published materials will contain due copyright acknowledgements for any third party materials contained within them.

10. Use of the school's Internet facility by visitors and guests

Members of school staff are expected to take responsibility for the actions of any adult guests or visitors who they allow or encourage to use the school Internet facilities. The essential "dos and don'ts" are explained to such visitors and guests prior to their use of the Internet. Unacceptable use will lead to the immediate withdrawal of permission to use the school Internet facility.

11. Responding to Incidents of Inappropriate or undesirable Use

11.1 Unintentional exposure of children to Inappropriate Content

It is the School's policy that every reasonable step should be taken to prevent exposure of children to undesirable materials on the Internet. It is recognised that this can happen not only through deliberate searching for such materials, but also unintentionally when a justifiable Internet search yields unexpected results.

If any users discover undesirable sites, the URL (web address) and content must be reported to the Head of School who will inform the Network Manager as soon as possible

11.2 Intentional access of undesirable Content by children

Children should never intentionally seek offensive material on the Internet. Such incidents will be treated as a disciplinary matter, and the parents of a child or children will be informed.

In the event of children being exposed to undesirable materials, the following steps will be taken:

- pupils will notify a teacher or teaching assistant immediately
- initially the Head of School will be notified by the teacher, and then the Executive Head Teacher as the designated safeguarding officer.
- the County approved forensic monitoring software will be used to investigate as appropriate (Smoothwall)
- parents will be notified at the discretion of the Executive Headteacher according to the degree of seriousness of the incident (for example, exposure to materials that include common profanities might not be notified to parents, but exposure to materials that included pornographic images would be notified)

11.3 Intentional access to undesirable Content by adults

Deliberate access to undesirable materials by adults is unacceptable, and **will be treated as a disciplinary issue.** If abuse is found to be repeated, flagrant or habitual, the matter will be treated as a very serious disciplinary issue. The Governors will be advised and the LA will be consulted. The County Council guidance regarding what to do with computers which have been used inappropriately will be followed in cases of serious misuse.

12. Disposal of ICT equipment

Will conform to:
The Waste Electrical and Electronic Equipment Regulations 2006
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Data Protection Act 1998
http://www.ico.gov.uk/what_we_cover/data_protection.aspx

Electricity at Work Regulations 1989
http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

13. Related documents

Acceptable Use Agreements and Protocols

- pupils' acceptable use agreements – shared with parents (Appendix A: EYFS/KS1 Appendix B: KS2 & KS3)
- adults (eg. staff, visitors and governors' user agreements) (Appendix C)
- parents' information leaflets
- EYFS/KS1 and KS2 online safety posters (versions of user agreements for display)
- Online safety Incident Log (Futures Digital)
-

School online safety resources

- Online safety education programme
- Online safety information on school website

School Safeguarding policy
Keeping Children Safe in Education – September 2021
Data Protection Policy
Behaviour policy
Anti-bullying Policy
Curriculum Policy

http://www.ceop.gov.uk/
http://clickcleverclicksafe.direct.gov.uk/index.html
http://www.thinkuknow.co.uk/default.aspx
http://searchenginewatch.com/showPage.html?page=2156191
http://www.wmnet.org.uk/21.cfm?zs=n

Guidance materials
www.becta.org (available via National Archives)

- Online safety: Developing whole school policies to support effective practice, Becta 2005
- Signposts to online safety: teaching online safety at KS1 and 2, Becta 2007