The Drive Community Primary School

Online Safety and Acceptable Use Policy Statement

September 2019

Rationale:

The potential that technology has to impact on the lives of all people increases year on year. This is probably even truer for children, who are generally much more open to developing technologies than adults. In many areas, technology is transforming both the way schools teach and children learn. At home, technology is changing the way children live and the activities in which they choose to partake. These trends are set to continue. While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- 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, which may constitute as abuse that may take place wholly online, or technology may be used to facilitate offline abuse. Children may be abused by an adult or adults or by another child or children. *(See Section 5: Abuse, in the Safeguarding Policy)*
- Access to unsuitable video / internet games Online sexual harassment, which might include: non-consensual sharing of sexual images / videos and sharing sexual images and videos (both often referred to as sexting); inappropriate sexual comments on social media; exploitation; coercion and threats. *(See also Appendix I: Sexually Harmful Behaviour in The Safeguarding Policy)*
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use, which may impact on social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we help those who work with our children beyond the school

environment (parents, friends and the wider community) to be aware and to assist in this process.

Policy and Leadership:

All at The Drive Primary School are committed to safeguarding children in our care. This policy has been developed by the E-Safety / Computing Co-ordinator and the Senior Leadership Team in order to ensure that it truly reflects our robust and thorough approach to safeguarding. This section outlines responsibilities of staff, leaders and stakeholders as well as all users of technology within school.

Responsibilities of the E-Safety / Computing Co-ordinator:

Our e-safety coordinator is the person responsible to the head teacher and governors for the day to day issues relating to e-safety. The e-safety coordinator:

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an safety incident.
- Provides training and advice for staff.
- Liaises with the Local Authority where necessary.
- Liaises with school IT technical support to ensure that internet access is appropriately filtered.
- Receives reports of e-safety incidents and maintains a log of incidents to inform future e-safety developments.
- Monitors and checks the forensic software reports weekly.
- Attends relevant meetings and committees of Governing Body.
- Reports regularly to Senior Leadership Team.
- Receives appropriate training and support to fulfill their role effectively.

Responsibilities of Governors:

Governors are responsible for ensuring that this policy is reviewed and enforced effectively.

Responsibilities of Head Teacher:

The Head Teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety is

delegated to the E-Safety / Computing Co-ordinator. The Head Teacher and the Deputy Head Teacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

Responsibilities of Classroom Based Staff:

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices and they participate in annual E-Safety training for all staff.
- They have read, understood and signed the school's Acceptable Use Policy for staff.
- They report any suspected misuse or problem to the E-Safety Co-ordinator.
- E-safety issues are embedded in the curriculum and other school activities.
- Policy Development, Monitoring and Review:
- This E-Safety Policy has been developed by a working party made up of:
- E-safety / Computing Co-ordinator
- Senior Management Team
- The implementation of this E-Safety policy will be reviewed by The E-Safety / Computing Co-ordinator. The e-safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

Policy Scope:

This policy applies to all members of the school 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 head teachers, to such extent as is reasonable, to regulate the behaviour of 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 school 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.

Acceptable Use Policies:

All members of the school community are responsible for using the school IT systems in accordance with the appropriate Acceptable Use Policy (AUP). AUPs are in place for staff, children (and their parents / carers) and volunteers in school and set out the expectations of all stakeholders when using school IT equipment. As part of their induction, any new member of staff is given the appropriate AUP and current AUPs are reviewed as needed in order to ensure that the policy within reflects the most recent developments in technology. The AUP is discussed with children as part of the E-Safety education within the Computing curriculum of study and copies are sent home to enable parents / carers to discuss the expectations with their children and support the school in providing a safe learning environment.

Illegal or Inappropriate Activities and Related Sanctions:

The school believes that the activities listed below are inappropriate in a school context **(those in bold are illegal)** and that users should not engage in these activities when using school equipment or systems (in or out of school). Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- **Child sexual abuse images (illegal - The Protection of Children Act 1978).**
- **Grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003).**
- **Possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008).**
- **Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986).**
- Pornography.
- Promotion of any kind of discrimination.
- Promotion of racial or religious hatred.
- Threatening behaviour, including promotion of physical violence or mental harm.
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.

Additionally, the following activities are also considered unacceptable on ICT equipment provided by the school:

- Using school systems to run a private business.
- Use of systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords).
- Creating or propagating computer viruses or other harmful files.
- Carrying out sustained or instantaneous high-volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet.
- On-line gambling and non-educational gaming.
- Use of personal social networking sites / profiles for non-educational purposes.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour management procedures.

Use of Hand-Held Technology (personal phones and hand-held devices):

We recognise that the area of mobile technology is rapidly advancing, and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- Members of staff are permitted to bring their personal mobile devices into school. Devices should only be used by members of staff in areas not accessed by pupils and only when not in contact with pupils. Staff can, however, request permission to keep a phone switched on in certain circumstances (e.g. an expected and important phone call).

- Older pupils are permitted to bring their personal hand-held devices into school with the agreement of parents (usually to facilitate the process of children beginning to walk home alone). All pupil phones are kept locked away during the school day and are collected by children before they leave.

Email:

Access to email is provided for all staff in school via Microsoft Outlook. These official school email services may be regarded as safe and secure and are monitored.

- Users need to be aware that email communications may be monitored.
- Users must immediately report, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

Use of Digital and Video Images:

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites. Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; the personal equipment of staff should not be used for such purposes. Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Pupils must not take, use, share, publish or distribute images of others without their permission.

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Head Teacher & ICT leader will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Parents or carers will be asked to notify school if they DO NOT wish for photographs or work of pupils to be published on the school Web site (letter see appendix 1).
- Pupil's learning outcomes can only be published with the permission of the pupil and parents.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Use of Web-based Publication Tools:

Our school has its own website for sharing information with the community beyond our school. This includes celebrating work and achievements of children. All users are required to consider good practice when publishing content. Personal information should not be posted on the school website. Photographs are posted but never include names alongside an image to identify a pupil. Full names are only used when no image could identify specific pupils.

Filtering:

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so (see appendix 2). It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

The school's internet is protected by a Firewall managed by the authority and any failure must be reported immediately. In addition, school has forensic software that reports the use of inappropriate language and search engines.

Responsibilities:

The day-to-day responsibility for the management of the school's filtering policy is held by the E-safety / Computing Co-ordinator (with ultimate responsibility resting with the head teacher and governors). They manage the school filtering, in line with the processes outlined below and keep logs of changes to and breaches of the filtering system. All users have a responsibility to report immediately to class teachers / E-Safety / Computing Coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should be blocked. Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education / Training / Awareness:

Pupils are made aware of the importance of filtering systems through the school's E-Safety Education Programme. Staff users will be made aware of the filtering systems through:

- Receiving and agreeing to the AUP and code of conduct
- Briefings in staff meetings, training days, memos etc. (from time to time and on-going).
- Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through E-Safety awareness sessions / newsletter etc.

Monitoring:

No filtering system can guarantee 100% protection against access to unsuitable sites. The Local Authority on behalf of the school will therefore monitor the activities of users on the internet.

E-Safety Education:

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in E-Safety is therefore an essential part of the school's computing

provision. Children and young people need the help and support of the school to recognise and avoid E-Safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them. E-Safety education will be provided in the following ways:

A planned e-safety programme should be provided as part of Computing lessons and should be regularly revisited – this will cover both the use of IT and new technologies in school and outside school.

- We use the resources on CEOP's Think U Know site as a basis for our E-Safety education.
- Key E-Safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of IT both within and outside school.
- In lessons, where internet use is pre-planned, it is best practice that 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, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- E-safety sessions are taught as part of the Kidsafe Programme.
- Information literacy: Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:
- Cross checking references (can they find the same information on other sites).
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are taught how to make best use of internet search engines to arrive at the information they require.
- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.

- Pupils will be informed that network and Internet use will be monitored.
- A record will be kept of any incidents of children accessing inappropriate websites. (see appendix 3)

It is our general school policy to require children to play a leading role in shaping the way our school operates and this is very much the case with our e-learning strategy. Children often use technology out of school in ways that we do not in school and members of staff are always keen to hear of children's experiences and how they feel the technology, especially rapidly developing technology (such as mobile devices) could be helpful in their learning. Pupils play a part in monitoring this policy.

Staff Professional Development:

It is essential that all staff receive E-Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff should receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy and acceptable use policies which are signed as part of their induction.
- The E-Safety Coordinator will receive regular updates through attendance at local authority or other information / training sessions and by reviewing guidance documents released by the DfE, local authority and others.
- All teaching staff have been made aware of this E-Safety policy and their responsibility to apply it.
- The E-Safety / Computing Coordinator will provide advice, guidance and training as required to individuals as required on an on-going basis.
- Governor training:
- Governors should take part in e-safety training / awareness sessions. This may be offered in a number of ways:
- Attendance at training provided by the external providers: National Governors Association or other bodies.
- Participation in school training / information sessions for staff or parents.
- Parent and carer awareness raising:

Many parents and carers have only a limited understanding of E-Safety risks and issues, yet they play an essential role in the education of their children and in the

monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site.
- Open evenings.
- Reference to the parent's materials on the Think U Know website (www.thinkuknow.co.uk) or others
- Drop in sessions led by the E-Safety / Computing Co-ordinator.

APPENDIX 1

The Drive Community Primary School
Photograph/Video/Social Media Permission

Name of Child:……
Class: ……

Occasionally, we may take photographs of activities that involve the children. The images may be used for displays, the school prospectus, our website or other publications by the Local Authority or local newspapers.

Photography or filming will only take place with permission of the Head teacher and under appropriate supervision. When filming or photography is carried out by the news media, children will only be named if there is a particular reason to do so (e.g. they have won a prize) and home addresses will never be given out. Images that might cause embarrassment of distress will not be used nor will images be associated with material on issues that are sensitive.

Before the school can take any photographs of your child we need your permission. Please answer the questions below, sign and date the form and return it to the school as soon as possible.

To comply with the Data Protection Act 1998 and the new General Data Protection Regulation (May 2018), we need to ask your consent before the school or the media record any images of your child. In view of this, please read the Statement below, complete the slip and return it to school within the next 10 days.

	YES	NO
May we use your child's photograph in the school prospectus and other printed publications that we produce for promotional purposes or on project display boards?		
May we use your child's image on our twitter/website		
May we record your child's image on video or webcam?		
Are you happy for your child to appear in the media?		
Your child's first name may appear with the image in the media.		

There may be other circumstances, which fall outside the normal day to day activities in the School, where pictures of the children are requested. We recognise that in such circumstances specific consent from the parent will be required before photography or filming can be permitted.
Please note that websites can be viewed throughout the world and not just in the United Kingdom where UK law applies.

I understand and agree / I understand and do not agree* to give consent.

IMPORTANT - I understand and agree / I understand and do not agree* that I can withdraw consent at any time and that permission will remain in force until parental permission is withdrawn or amended.

Signature of Person Responsible for the Chid:
……

*delete as applicable

Relationship to child:
……

Address:
……
……

Telephone number:
……

Date: ……

APPENDIX 2

The Drive Community Primary School
Consent Form for Responsible Internet Access

Name of Child: …… Class: ……

I understand that children will always be supervised whilst using the internet and give permission for my son/daughter to access the Internet.

I understand that the school will take all responsible precautions to ensure that 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 the use of the Internet facilities.

To comply with the Data Protection Act 1998 and the new General Data Protection Regulation (May 2018), we need to ask your consent before children participate in any such activities above. In view of this, please read the Statement below, complete the slip and return it to school within the next 10 days.

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 the use of the Internet facilities.

I agree / I do not agree that I have read and understood the School Rules for Responsible Internet Access.

IMPORTANT - I understand and agree / I understand and do not agree* that I can withdraw consent at any time and that permission will remain in force until parental permission is withdrawn or amended.

Signature of Person Responsible for the Chid:

……

*delete as applicable

Relationship to child:

……

Address:

……

……

Telephone number:

……

Date: ……

APPENDIX 2

THE DRIVE PRIMARY SCHOOL

Logging system for inappropriate Internet Sites and Usage

Date	Website	Child Name and Parent Informed	Reported To E-Safety Leader	Reported to Head Teacher	Actions (e.g. LA informed and Website blocked)