Online Safety

Policy Statement 2018-2021

Every child has the right to an education (Article 28).
You have the right to be protected from being hurt and mistreated, in body or mind (Article 19)
No one is allowed to punish you in a cruel or harmful way (Article 37)
UN Convention on the Rights of the Child

1. Rationale:

1.1 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.
- Access to unsuitable video / internet games.
- 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.

1.2 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.

2. Policy and Leadership:

2.1 All at Harlow Green Community Primary are committed to safeguarding children in our care. This policy has been developed by the Online Safety / Computing Leader 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.

3. Responsibilities of the Online Leaders/ co-ordinators:

3.1 Our online safety leaders are:

- Headteacher
- Deputy Head Teacher
- Computing Leader
- IT Technician

3.2 These leaders:

- Take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the online safety policies / documents.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident.
- Provide training and advice for staff.
- Liaise with the Local Authority where necessary.
- Liaise with school IT technical support to ensure that internet access is appropriately filtered.
- Receive reports of online safety incidents and maintains a log of incidents to inform future online safety developments.
- Attend relevant meetings and committees of Governing Body.
- Report regularly to Senior Leadership Team.
- Receive appropriate training and support to fulfil their role effectively.

4. Responsibilities of Governors:

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

5. Responsibilities of Head Teacher:

5.1 The Head Teacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety is delegated to the Online Safety / Computing Leaders. The Head Teacher and the Deputy Head Teacher should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

6. Responsibilities of classroom based staff:

6.1 Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices and they participate in annual Online 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 Online Safety Co-ordinator.
- Online safety issues are embedded in the curriculum and other school activities.

7. Policy Development, Monitoring and Review:

7.1 This Online Safety Policy has been developed by a working party made up of:

- Online safety / Computing Co-ordinator
- Senior Management Team

The implementation of this Online Safety Policy will be reviewed by	The Online Safety / Computing Coordinator.
Monitoring will take place at regular intervals	Annually.
The governing body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of any online safety incidents) at regular intervals	Termly via the Head Teacher's Report to Governors
The online safety policy will be reviewed every three years, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.	

8. Policy Scope

8.1 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 online 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 online safety behaviour that take place out of school.

9. Acceptable Use Policies:

9.1 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 Online 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.

10. Illegal or inappropriate activities and related sanctions:

10.1 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.

10.2 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.
- Online line gambling and non-educational gaming.
- Use of personal social networking sites / profiles for non-educational purposes.

10.3 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.

11. Use of hand held technology (personal phones and hand held devices):

11.1 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 on 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).
- Mobile phones must not be kept out in view of pupils and must be kept securely out of sight unless when being used in the above areas.
- Staff are permitted to use their own mobile phones on school trips, PE / sport events and when communicating around school across the campus site. They must be kept out of sight of children and other parent helpers etc.
- Staff should never use their own personal mobile devices to take or store photographs of children at school events, sporting trips or excursions. Only authorised school cameras and iPads can be used to record videos or images of school events.
- 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.

12. E mail:

12.1 Access to email is provided for all staff in school via Microsoft Outlook. These official school 2email 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.

13. Use of digital and video images:

13.1 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.

14. Use of web-based publication tools:

14.1 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.

15. Filtering:

15.1 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. Our school filtering is managed and maintained by the local authority who are responsible for blocking, filtering and unblocking any requested websites.

16. Responsibilities:

16.1 All users have a responsibility to report immediately to class teachers / Online 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.

17. Education / training / awareness:

17.1 Pupils are made aware of the importance of filtering systems through the school's Online 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).

17.2 Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through Online Safety awareness sessions / newsletter etc.

18. Monitoring:

18.1 No filtering system can guarantee 100% protection against access to unsuitable sites. The Local Authority on behalf of the school can monitor the activities of users on the internet. In addition, at Harlow Green we use Impero software, which allows us to monitor all users on a daily basis. All concerns are logged and investigated and the Headteacher or Deputy Headteacher is informed.

19. Online Safety education:

19.1 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 Online 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 Online 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. Online Safety education will be provided in the following ways:

- A planned online 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 Online Safety education.
- Key Online 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.
- Online safety sessions are taught as part of the Kidsafe Programme.

20. Information literacy:

20.1 Pupils should be taught in all lessons to be critically aware of the content they access online 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.

20.2 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 online 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.

21. Staff Professional Development:

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

- A planned programme of formal Online Safety training will be made available to staff.

- All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and acceptable use policies which are signed as part of their induction.
- The Computer Leader 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 Online Safety policy and their responsibility to apply it.
- The Online Safety / Computing Leader will provide advice, guidance and training as required to individuals as required on an on-going basis.

22. Governor training:

22.1 Governors should take part in online 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.

23. Parent and carer awareness raising:

23.1 Many parents and carers have only a limited understanding of Online 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 online 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, website.
- Open evenings.
- Reference to the parents materials on the Think U Know website (www.thinkuknow.co.uk) or others
- Drop in sessions led by the Online Safety / Computing Leader or other agencies.