Overton CE Primary School

E-Safety Policy

September 2023

1. Introduction

Overton CE Primary School recognises the benefits and opportunities, which new technologies offer to teaching and learning. We encourage the use of technology in order to enhance skills and promote achievement. However, the accessible and global nature of the internet and variety of technologies available mean that we are also aware of potential risks and challenges associated with such use. This policy sets out how we strive to keep children safe with technology while they are in school, providing a curriculum, which prepares children for the digital world. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we 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 attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process. This e-safety policy should be read in conjunction with other relevant school policies e.g. safeguarding procedures, Safer Working Practices, Anti Bullying, Prevent Duty and Child Protection.

2. Creation, Monitoring and Review

The school e-Safety Policy has been written by the Computing Team Leader and passed to the Leadership Team and Governors to be reviewed and accepted as a policy. The impact of the policy will be monitored regularly with a full review being carried out every 2 years. The policy will also be reconsidered where concerns are raised by members of the school staff, pupils or Governors or where an e-safety incident has been recorded.

3. Policy Scope

The policy applies to all users of the school community who have access to the school IT systems, both on the premises and remotely. Any user of school IT systems must adhere to and sign a hard copy of the Acceptable Use Policy/AUP (see appendix 1). The e-Safety Policy applies to all use of the internet and electronic communication devices such as email, Internet Explorer, mobile phones, games consoles, iPads, social networking sites and instant messaging. 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 cyberbullying 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 antibullying policies and will, where known, inform parents / carers of incidents of inappropriate esafety behaviour that take place out of school

4. Roles and Responsibilities

All members of the school should know who is responsible for e-safety. It should be clear to whom they can report concerns or gain further information. There are clear lines of responsibility for e-safety within the school. For pupils the first point of contact should be their teacher or mentor. All staff are responsible for ensuring the safety of pupils and should report any concerns immediately to one of the Designated Safeguarding Leaders (DSLs) in regards to a specific safeguarding concern. When informed about an e-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved. Where any report of an e-safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where management considers it appropriate, the Designated Safeguarding Leader may be asked to intervene with appropriate additional support from external agencies.

Responsibilities: Governors

Our Governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the Governors (or a Governors' subcommittee) receiving regular information about e-safety incidents and monitoring reports

Responsibilities: Head Teacher

The Head Teacher is responsible for ensuring the safety (including e-safety) of members of the school community. The Head Teacher and another member of the Leadership team 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. (see Figure 1)

Responsibilities: classroom based staff

Teaching and Learning 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. They have read, understood and signed the school's Acceptable Use Policy for staff (see appendix 1) and must actively promote this through embedded good practice. Digital communications with pupils (email / learning platform/ voice) should be on a professional level and only carried out using official school systems. Contact with pupils through social networking sites and instant messaging is prohibited. E-safety teaching is embedded in the school's curriculum and other school activities. E-safety is considered of paramount importance whilst setting and receiving online remote learning always – in addition, outlining the need for parental permissions when accessing websites such as YouTube or joining on Microsoft Teams for example. They adhere to this policy alongside the school's Safeguarding and Remote Education policies

5. Security

The school will do all that it can to make sure the school network is safe and secure, but not so secure that it gets in the way of learning. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of school systems and information.

Filtering

At present our school network is filtered directly from Hampshire County Council. If an inappropriate image or website is not blocked staff must report this straight away to Computing team/SLT who will then contact Hampshire County Council to see that it becomes filtered.

6. Behaviour Online

Communication can take many forms, whether it is by email, text, video conferencing or instant chat. It is essential that all pupils and staff are aware of existing school policies that refer to acceptable behaviours when communicating online. Overton CE Primary School will ensure that all users of technologies adhere to the standard of behaviour as set out in the Acceptable Use Policy. The school will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and pupils should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the appropriate student and staff disciplinary policies. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police

7. Acceptable Use Policies (AUP)

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to school systems. Acceptable use policies are provided in Appendix 1 of this policy for:

- Pupils (EYFS + KS1 / KS2)
- Staff (and volunteers)
- Parents / carers (including permissions to use pupil images / work and to use ICT systems)

Acceptable use policies are revisited and revised annually at the start of each school year and amended accordingly in the light of new developments and discussions with the children which take place at the time. Copies are available on the school website. For children in EYFS and KS1 parents may sign on behalf of their children. Staff and volunteers sign when they take up their role in school and in the future if significant changes are made to the policy. Parents sign once when their child enters the school. The parents' policy also includes permission for use of their child's image (still or moving) by the school, permission for their child to use the schools ICT resources (including the internet) and permission to publish their work. Community users sign when they first request access to the school's ICT system. Induction policies for all members of the school community include this guidance.

8. Illegal or inappropriate activities.

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:

- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Hampshire County Council and / or 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 (e.g. 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

9. Sanctions

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 / disciplinary procedures.

10. Procedures

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

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

Please refer to the Overton CE Primary School Mobile Phone Policy on our school website for further information regarding the use of hand held devices by staff and pupils. This policy is also included in the school's staff handbook.

12. Email

Access to email is provided for all staff in school via the intranet page accessible via the web browser (Internet Explorer) from their desktop. These official school email services may be regarded as safe and secure and are monitored.

- Staff use only the school email services to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- A structured education programme is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email.
- Users must immediately report, to the e-safety Team Leader – 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

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.

Whilst conducting remote learning; audio, video and photographs may be recorded and uploaded by both children and staff through the Seesaw/Tapestry platforms only. See also the following section for guidance on publication of photographs.

14. Use of web-based publication tools

Our school uses the public facing website, www.overtonprimary.co.uk for sharing information with the community beyond our school. This includes, from time-to-time 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 and only official email addresses (provided as links rather than appearing directly on the site) should be used to identify members of staff (never pupils).
- Only pupils' first names are used on the website, and only then when necessary.
- Detailed calendars are not published on the school website.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
- Pupils' full names will not be used anywhere on a website, and never in association with photographs. Permission from parents or carers will be obtained

before photographs of pupils are published on the school website, in line with the AUP agreement.

15. 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 e-safety provision. Children 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 is provided as part of Computing, PSHE and other lessons and is regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. It is also recommended to take place during the first part of each Computing session.
- We use the resources such as CEOP's Think U Know site to support our e-safety education http://www.thinkuknow.co.uk/teachers/resources/ (Hector's World at KS1 and Cyber Caf at KS2)
- Learning opportunities for e-safety are built into the school curriculum for Computing.
- Key e-safety messages are reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
- Children are helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT both within and outside school.
- In lessons where internet use is pre-planned, children are 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 children are allowed to freely search the internet, e.g. using child friendly search engines such as 'swiggle', staff are vigilant in monitoring the content of the websites our children visit.
- Whilst children are conducting remote learning ensure that they are instructed to do so safely and reminded of safe searching and E-Safety expectations.

16. Social Media

As a school we recognise that social media and networking are playing an increasing role within everyday life and that many staff, governors and parents are users of tools such as Facebook, Twitter and blogs using these for both personal and professional use. We ensure that staff, Governors and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks.

As a school we block access to social networking sites on all school computers.

Staff and Governors:

- Ensure that their profile/posts are kept private to friends where possible, this also includes personal information such as phone numbers, email addresses etc.
- Do not accept current or ex-pupils as 'friends' on social media sites such as Facebook whilst they are of school age. This is to ensure any possible misinterpretation. We do understand that some staff members live and have friends within the local community and ask that these members of staff take extra care when posting online.
- Ensure that their communications and publications maintain their professionalism at all times and does not undermine the professional reputation of themselves or the school. Staff are to only use the school email system to make contact with multi-agencies. Any staff/parent communication should go through the administration team if not in link books: adminoffice@overton.hants.sch.uk
- Are aware that electronic texts can be misconstrued so should only be used to communicate instructional / temporal information
- Will not use these media to discuss confidential information or to discuss specific children
- Check with the IT Team Leader if they need advice on monitoring their online persona and checking their security settings. Pupils should not be signed up to most social networking sites due to 13+ age guidelines. As a school we will monitor the use of social networking and ensure it is part of our curriculum. We will ensure that parents are aware of the age restrictions on social media sites and of the potential dangers of children using these sites as well as how to minimise the risk if their children are using them. As a school, we do reserve the right to contact sites such as Facebook and ask them to remove our children's accounts, if sites are used inappropriately (such as cyber-bullying, posting personal information). Where safeguarding concerns arise, the school will respond to these in line with existing policies (e.g. Anti-Bullying Policy, Child Protection, Behaviour Policy) As a school we may introduce blogging in the future. If this is the case we shall amend this policy to provide guidelines in how this shall be used.

17. Cyber Bullying

Online bullying and harassment Online bullying and harassment via Instant messaging, mobile phone texting, e-mail and chat rooms are potential problems that can have a serious effect on pupils. Our school has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy. These include:

- No access to public chat-rooms, Instant Messaging services and bulletin boards.
- Pupils are taught how to use the Internet safely and responsibly, and are given access to guidance and support resources from a variety of sources. We encourage pupils to discuss any concerns or worries they have about online bullying and harassment with staff, and have a range of materials available to support pupils and their families.
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy found on our school website.
- Complaints related to child protection are dealt with in accordance with school child protection procedures.

18. Information literacy

Pupils will 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:

- Checking the likely validity of the URL (web address)
- Cross checking references (can they find the same information on other sites)
- Checking the pedigree of the compilers / owners of the website
- 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.

We use the resources on CEOP's Think U Know site as a basis for our e-safety education as well as resources from:

- NSPCC (www.nspcc.org.uk/keeping-children-safe/online-safety/)
- Thinkuknow (www.thinkuknow.co.uk/)
- Hectors world (www.esafety.gov.au/educators/classroom-resources/hectors-world)
- Using safe search engines such as 'Kiddle' and 'Swiggle'

19. Staff training

All staff receive regular e-safety training, both in-house and from external expert providers, and understand their responsibilities, as outlined in this policy.

Training is offered as follows:

- A planned programme of formal e-safety training is made available to staff. An audit of the e-safety training needs of all staff will be carried out annually.
- It is expected that some staff will identify e-safety as a training need within the performance management process.
- 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. Our Computing team leads this.
- The E-Safety Team Leader will receive and disseminate regular updates through attendance at local authority or other information / training sessions and by reviewing guidance documents released by the DfE, local authority, the HSCB (Hampshire Safeguarding Children's Partnership) and others.
- All teaching staff have been involved in the creation of this e-safety policy and are therefore aware of its content
- The Computing team will provide advice, guidance and training as required to individuals as required on an on-going basis.
- The E-Safety Team Leader will ensure all staff are aware of the remote learning policy and support to ensure they are accessing Seesaw/Tapestry platforms safely and securely.

20. Parent and carer awareness

Parents and carers may have 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, email, texts and via our website
- Parents' evenings, expectation meetings and information workshop meetings
- Reference to the parents' materials on the Think U Know website (www.thinkuknow.co.uk) or and through regularly updated information found on our website www.overtonprimary.co.uk

In order to support their child, parents and carers should:

- Read the school AUP, encourage themselves and their children to adhere to them
- Discuss online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home
- Role model safe and appropriate uses of technology and social media
- Identify changes in behaviour that could indicate that their child is at risk of harm online
- Refer to the remote learning policy whilst completing remote learning.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.

Professionals CEOP (Child Exploitation and http://www.ceop.police.uk/safety-centre Online Protection)

Safety Centre Childnet International http://www.childnet.com

Know IT All http://www.childnet-int.org/kia/

Professionals Online Safety Email helpline@saferinternet.org.uk or telephone Helpline (UKSIC) 0844 381 4772

SWGfL Staying-Safe (South http://www.swgfl.org.uk/Staying-Safe West Grid for Learning)

Think U Know (CEOP) http://www.thinkuknow.co.uk/

UK Safer Internet Centre http://www.saferinternet.org.uk (UKSIC)

Children, Young People & Families A Parent's Guide to Technology http://www.saferinternet.org.uk/advice-and-resources/a-parents-guide

Connect Safely http://www.connectsafely.org

Digizen http://www.digizen.org

KidSmart http://www.kidsmart.org.uk/

Get Safe Online http://www.getsafeonline.org/

Know IT All http://www.childnet-int.org/kia/parents/

Think U Know http://www.thinkuknow.co.uk/

Appendix 1

ICT Acceptable Use Agreement for Staff

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's policy for Internet access for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I understand that I must not use the school ICT system to access inappropriate content
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems and hardware may not be used for private purposes without specific permission from the Head Teacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely. It must NOT be kept on removable storage devices.
- I will respect copyright and intellectual property rights.
- I understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- I will report any incidents of concern regarding children's safety to the schools e-Safety Coordinator, the Designated Child Protection Liaison Officer or Head Teacher.
- I will ensure that electronic communications with pupils including email, Instant Messaging and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing. The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing

unauthorised or unlawful text, imagery or sound. I have read, understood and accept the Staff Code of Conduct for ICT.

Signed: ……………………………… Capitals: ……………………… Date: ………

Accepted for school: ……………… Capitals: ………………………….

ICT Acceptable Use Agreement for Pupils E-Safety Rules

Key Stage 1

Think then Click

These rules help us to stay safe on the Internet:

- We only use the internet when an adult is with us.
- We can send and open emails together.
- We always ask if we get lost on the Internet.
- We can click on the buttons or links when we know what they do.
- We can write polite and friendly emails to people that we know.
- I know I should never share personal information like my name, address or passwords with anyone.
- I know that if I see anything online that I don't like or understand I will tell and adult.

Key Stage 2

Think then Click

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We only use safe search sites when browsing.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any web page we are not sure about.
- We only message or email people an adult has approved.
- We send e-mails or messages that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails or messages sent by anyone we don't know.
- We do not use Internet chat rooms.
- We only use age appropriate apps.
- We try hard to keep our identity safe online.