Old Hutton
C of E Primary School
Learning for life

Learning for Life 'in all its fullness' (John 10:10)

'So we fix our eyes not on what is seen, but on what is unseen, since what is seen is temporary, but what is unseen is eternal' (2 Corinthians 4:18)

ONLINE SAFETY POLICY & PROCEDURES

Designated Safeguarding Lead (DSL)	Fiona Hadwin
Deputy Designated Safeguarding Lead (DSL)	Andrea Walker

Approved by	
Name:	
Position:	
Signed:	
Date:	January 2021
Review date:	January 2022

Policy overview

The purpose of this policy is to safeguard and protect all members of Old Hutton C of E Primary School online community by providing a framework to promote and maintain a safe, effective and responsive online safety culture. The policy is applicable to all members of Old Hutton Primary and includes staff, students and pupils, volunteers, parents/carers and visitors who have access to our digital technology systems, both internally and externally.

Key references – other documents to be read to support this policy

- Our School Google Classroom Pupil (& Parent) User Agreement
- Our School ICT Staff/Volunteer Acceptable Use Agreement
- Our School Child Protection & Safeguarding Policy & Procedures – especially Section 20: Online safety
- Department for Education (DfE) (2020) Keeping Children Safe in Education: statutory guidance for schools and colleges. Annex C: Online Safety
- Department for Education (DfE) (2019) Teaching online safety in school

Our Online Safety School Statement

Old Hutton School aims to **educate and protect** our whole school community in its use of technology. We assert that:

- online safety is an essential element of safeguarding and we have a statutory obligation to ensure that all learners and staff are protected from potential online harm;
- ICT (Information Communication Technology), including use of devices and the internet, is an integral, important and constantly evolving part of everyday life; all learners should be empowered to build their knowledge, skills and resilience in its use and to develop strategies to recognise and respond to online risks;
- we will ensure a comprehensive curriculum response to educate and enable all learners to develop their digital literacy, including awareness and effective management of the associated risks; we will support staff and parents/carers to be alert to the needs of keeping children safe online and of keeping up-to-date with new technologies and risks;
- we have mechanisms in place to identify, intervene in and escalate any incident where appropriate.

Online safety definitions

'Online abuse is any type of abuse that happens on the web/internet, whether through social networks, playing online games or using mobile phones' (NSPCC, 2019).

The use of technology has become a significant component of many safeguarding issues, providing a platform that can facilitate harm (e.g. bullying, radicalisation, child sexual exploitation and predation). The breadth of issues classified within online safety is considerable, but can be categorised into 3 main areas of risk:

- **contact:** contact from someone online who may wish to bully or abuse the child. This could also include other children or adults posing as children or young adults and involve threatening, stalking, online grooming, online harassment or activities of a commercial nature, including tracking and gathering person information;
- **content:** being exposed to inappropriate or illegal material online including: adverts, spam, sponsorship, personal info, violent or hateful content, racist or radical and anti-extremist views, pornographic or unwelcome sexual content, biased materials and misleading information or advice;
- **conduct:** the child may be the perpetrator of activities that increase the likelihood of or cause harm, including: illegal downloading, hacking, gambling, bullying or harassing another child or adult. They might create, send and receive inappropriate material e.g. explicit images (sexting) or provide misleading information or advice.

(Keeping Children Safe in Education, DfE 2020)

Roles and responsibilities

High quality online safety provision requires all stakeholders to be well-informed, constantly vigilant and ready to act when issues arise.

All Staff/Volunteers need to:

- always act in the best interests of the child;
- be aware of and adhere to the **Staff/Volunteer ICT Acceptable Use Policy Agreement** and policies/ procedures in school which support online safety and safeguarding;
- support in the ownership and responsibility for the security of systems and the data accessed;
- model good practice when using technology and educate learners in its use through the curriculum, being especially aware of the potential additional needs of vulnerable and SEND learners;
- know how to recognise, respond to and report signs of online abuse and harm and any concerns (see below);
- know the process for making referrals and reporting concerns (see below);
- receive appropriate training and updates in child protection and online safety, including policy/procedure review.

Governors and Headteacher/Senior Leadership are responsible for:

- upholding online safety as an essential element of safeguarding which is embedded across the whole school culture;
- ensuring that children are provided with a safe environment in which to learn and develop;
- ensuring that the school has risk-assessed and put in place appropriate securities, filters and monitoring systems on the internet (also to meet the requirements of the 'Prevent Duty'), online platforms and all school devices;
- ensuring the school has effective policies and training in place;
- auditing and evaluating online safety practice;
- ensuring there are robust reporting channels.

Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Lead (Deputy DSL) must:

- take responsibility for all safeguarding matters, including online safety and collaborate with Governors and Head in creation, evaluation and updating of policy and procedures;
- ensure children are being appropriately taught about and know how to use the internet responsibly;
- ensure teachers and parents/carers are aware of measures to keep children safe online through relevant information and training provision;
- facilitate effective record keeping and the reporting and monitoring of all online safety concerns (see below);
- promote online safety and the adoption of a whole school approach;
- maintain own training and learning needs, keeping up to date with all matters relating to online safety.

Children need to:

- know who the DSL is;
- engage in age-appropriate online safety education opportunities through our Computing and PSHCE/RSE curriculum;
- contribute to policy/procedure development and review through pupil voice activities;
- read, understand and adhere to online safety policy/procedures (our **Pupil Use Agreement**);
- respect the feelings of others, both off and online;
- take responsibility for keeping themselves and others safe online;
- know where and how to find help with any online incidents or concerns;
- how, when and where to report concerns and when to seek help from a trusted adult.

Parents and Carers:
Parents and carers need to understand the risks that children face online to protect them from online dangers. They need to:
- read and adhere to all relevant policies (this **Online Safety Policy**, our **Remote Education Provision** document, our **Google Classroom Pupil (& Parents) Use Agreement**);
- be responsible when taking photos/using technology at school events;
- know who the school DSL (Designated Safeguarding Lead) is;
- know how to report online issues (to the school, through a phone call or email via the office; depending on need, this could be addressed to the class teacher, Computing subject leader/Google Classroom Co-ordinator, DSL or Head teacher; and/or direct to the CEOP website www.ceop/police.uk/safety-centre);
- support online safety approaches and education provision, including ensuring that home devices, apps and programs accessed by their children have passwords/log-ins, age-appropriate parental controls activated and internet filters are in place on the home system to block malicious websites (see advice at www.saferinternet.org.uk/advice-centre/parents-and-carers and **Annex to Policy: Advice for parents** below);
- be a role model for safe and appropriate behaviour;
- identify changes in children's behaviour that could indicate they are at risk of online harm or abuse (see below).

Cultivating a safe environment – educate

At Old Hutton School, we address aspects of online safety through our Computing and PSHCE/RSE curriculum. Our learners will be educated in an age-appropriate way about:
- how to evaluate what they see online
- how to recognise techniques for persuasion
- their online behaviour
- how to identify online risks
- how and when to seek support.

Evaluate: how to evaluate what they see online
This will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable. We will help pupils to consider questions including:
- Is this website/URL/email fake? How can I tell?
- What does this cookie do and what information am I sharing?
- Is this person who they say they are?
- Why does someone want me to see this?
- Why does someone want me to send this?
- Why would someone want me to believe this?

Recognise: how to recognise techniques used for persuasion
This will enable pupils to recognise the techniques that are often used to persuade or manipulate others. A strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity. We will help pupils to recognise:
- online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation);
- techniques that companies use to persuade people to buy something;
- ways in which games and social media companies try to keep users online longer (persuasive design);
- criminal activities such as grooming.

Online Behaviour

This will enable pupils to understand what acceptable and unacceptable online behaviour looks like. At Old Hutton School, we will teach pupils that the same standard of behaviour and honesty applies online and offline, including the importance of respect for others. We will also teach pupils to recognise unacceptable behaviour in others. We will help pupils to recognise acceptable and unacceptable behaviour by:

- looking at why people behave differently online. For example, how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do;
- looking at how online emotions can be intensified resulting in mob mentality;
- teaching techniques (relevant on and offline) to defuse or calm arguments (for example, a disagreement with friends) and disengage from unwanted contact or content online;
- considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.

Identify: how to identify online risks

This will enable pupils to identify possible online risks and make informed decisions about how to act. This should not be about providing a list of what not to do online. The focus should be to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action. We will help pupils to identify and manage risk by discussing:

- the ways in which someone may put themselves at risk online;
- risks posed by another person's online behaviour;
- when risk taking can be positive and negative;
- "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations, i.e. how past online behaviours could impact on their future when applying for a place at university or a job for example;
- the risks vs the benefits of sharing information online and how to make a judgement about when and how to share and who to share with;
- the specific risks associated with taking, use, sharing, publication and distribution of digital images, including the risks attached to publishing their own images on the internet e.g. on social networks;
- and asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?

How and when to seek support

This will enable pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online. We will help pupils by:

- helping them to identify who trusted adults are and that it is first to a trusted adult they should go to if they are unhappy or upset by anything they see or hear online;
- looking at the different ways to access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations, such as Childline;
- helping them to understand that different platforms, devices and apps will have ways in which inappropriate contact or content can be monitored and reported.

Cultivating a safe environment – protect

Procedure for staff responding to online safety concerns

Child welfare is of principal concern – the best interests of children take precedence. If staff have any concerns about their own or others' online safety, have concerns shared with them by a child or other staff member, or feel that children may be at risk of online harm or abuse, this must immediately be reported. Immediate action may be required to safeguard investigations and any other children affected.

Most reporting follows the same procedure as explained in our child protection and safeguarding policy for any concerns about children:

- share with the DSL (Fiona Hadwin), Head teacher/ Deputy DSL (Andrea Walker) or if neither are available, our additional trained Deputy DSLs (Charlotte Harrison or Rachel Hayes)
- concerns should be recorded using the disclosure concern record sheet (available from the safeguarding file in the teachers' area on the school server or on the child protection notice board in the staffroom) and actioned, as decided by the DSL/Head teacher
- children will be enabled (at a level appropriate to their age and ability) to share online concerns
- actions may include contacting the LSCB Cumbria Safeguarding Hub or seeking health and safety advice from the Cumbria H&S team or our H&S adviser, Kym Allan
- any unsafe or worrying online issue can also be reported directly to the CEOP website www.ceop/police.uk/safety-centre
- If there is any immediate danger, contact the police on 999.

Procedure for responding to complaints about staff or concerns about other adults

If a complaint or allegation is made by a child or young person, parent/carer, member of the public or colleague about another staff member or other adult in relation to online safety, this should be referred to the DSL and Head teacher, who will ensure the complaint /allegation is recorded and actioned as required. This may involve, depending on the nature of the issue:

- following the school complaints policy and procedures and/or child protection and safeguarding policy and procedures
- seeking advice from the LSCB, Cumbria H&S team or our H&S adviser, Kym Allan
- enquiries and assessment by children's social care or adult social care relating to whether a child, young person or adult at risk is in need of protection or services
- consideration by an employer of disciplinary action in respect of the individual (including suspension)
- a police investigation of a possible criminal offence.

It is the responsibility of staff to inform the DSL and Head teacher if they are being investigated in relation to any child protection concerns, including regarding online safety, outside of work. They should also report if their own children/stepchildren/children they are living with become subject to child protection matters or an adult related to them or living with them becomes subject to adult protection matters.

Development of the Policy

This policy will be monitored and reviewed annually, or earlier in the light of any incidents or investigations, legislative changes or developments in best employment practice, to ensure its continuing relevance and effectiveness.

Annex: Advice for parents on keeping their children safe online

- Ensure you have read the school's **Pupil/Parent Use Agreement** for ICT and our online learning platforms (Google Classroom and Tapestry) and that you and your child understand and adhere to these agreed rules.
- Ensure you have read the school's **Remote Education Provision** information document.
- Start setting some boundaries, from an early age, to limit screen time.
- Supervise and monitor your child's use of devices and the internet; ensure that you know what they are using or watching. By visiting different websites, they may stumble across something inappropriate, as well as possibly causing devices to become infected with viruses.
- Talk to your children about their use of the internet; ensure they know that no-one has the right to make them do anything they do not want to do; check they understand what to do if they are worried or upset by anything they see or hear online (come off the screen; tell a trusted adult).
- Make sure devices like your mobile, tablet or laptop are out of reach. Set up passwords/PINs and make sure you keep these details to yourself.
- On computers and any other devices your child has access to, set the parental controls to the appropriate age, and enabling access to only appropriate content (see below).
- Buy or download parental control software, switch it on and keep it updated (see below).
- Internet Service Providers (ISPs) usually give their customers free parental controls which can be activated at any time. Check them out and take advantage of them.
- Buy or download only apps, games, online TV and films which have age ratings and check these before allowing your child to play with or watch them.
- Share your technology rules with grandparents, babysitters and your child's friends' parents so that they know what to do when looking after your child.
- When using public WiFi – e.g. in cafés or hotels – remember that it might not include parental controls. Innocently letting your child play with your mobile or tablet may result in them accessing inappropriate content or revealing personal information.

Among the most **common signs to watch out for** which may indicate potential online safety issues include children and young people who:

- become very/unusually secretive, especially about what they are doing online
- avoid discussions about what they are doing online
- are spending a lot of time on the internet and social media (beyond what is expected for school work)
- are switching screens on their device when approached
- are withdrawn or angry after using the internet or sending text messages or becomes unusually secretive
- have lots of new phone numbers or email addresses on their devices
- unexpectedly stops using their device(s)
- appear nervous or jumpy when using their device(s)
- appear to be angry, depressed, or frustrated after going online (including gaming)
- appear uneasy about going to school or outside in general
- may be oversleeping or not sleeping enough and may be having nightmares
- become abnormally withdrawn from friends and family members
- show an increase or decrease in eating
- make passing statements about suicide or the meaninglessness of life
- lose interest in the things that used to matter most to them.

Support and guidance
If you are concerned or have any questions on how to approach the subject with your children, please contact school and/or you can also access support from:

The National Crime Agency/CEOP safety centre for reporting online concerns www.ceop.police.uk/safety-centre

The Thinkyouknow website is CEOP's education programme, with lots of useful information for parents about how to make good use of the internet while staying in control thinkuknow.co.uk/parents

The UK Safer Internet Centre, through its excellent Parents' Guide to Technology, gives advice on safety tools, filters and how to set up controls on a device: www.saferinternet.org.uk/advice-centre/parents

The National Online Safety website at www.nationalonlinesafety.com has a series of Parent Guides (e.g. for smartphones, TikTok, Minecraft) which are very helpful for keeping up to date with the latest trends and providing safety tips and advice.

Visit www.internetmatters.org/parental-controls to find out how you can set up controls on your home internet, phone network and online services such as Netflix

Age-appropriate apps and games for young children to use by filtering by age at www.commonsensemedia.org

Childnet website www.childnet.com/parents-help

Children who are worried about their activity on apps or online games can contact Childline for advice 24 hours a day, online at www.childline.org.uk and over the phone on 0800 1111