



OLDFLEET PRIMARY SCHOOL

Online Safety Policy

Our Vision

All our children are buzzing with excitement for learning; they enjoy the feeling of success, develop confidence, and become active and responsible citizens.

Aims

These aims are for our whole school community – children, staff, governors and families:

- To develop independent, enthusiastic and creative learners with skills for life
- To provide a welcoming, happy and safe environment, where learners are confident to take risks and can flourish
- To deliver an authentic curriculum, which provides opportunities for challenge and aspiration, preparing children for the future
- To build a community based on mutual respect, where everyone takes responsibility for their own actions and behaviour choices
- To celebrate diversity and promote tolerance, developing learners as global citizens

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

Websites

Apps

Email, Instant Messaging and chat rooms

Social Media, including Facebook and Twitter

Mobile/ Smart phones with text, video and/ or web functionality

Other mobile devices including tablets and gaming devices

e-Safety Games

Learning Platforms and Virtual Learning Environments

Blogs and Vlogs

Podcasting

Video sharing

Downloading

On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

At Oldfleet Primary school, we understand the responsibility to educate our pupils on Online Safety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the

school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Online Safety

Online Safety in the Curriculum

ICT and Online resources are increasingly used across the curriculum. We believe it is essential for Online Safety guidance to be given to the pupils on a regular and meaningful basis. Online Safety is embedded within our curriculum and we continually look for new opportunities to promote Online Safety.

The school provides opportunities within a range of curriculum areas to teach about Online Safety

Educating pupils about the Online risks that they may encounter outside school is done informally when opportunities arise and as part of the Online Safety curriculum

Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them

Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities

Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of Online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or the 'CEOP report abuse' button

Online Safety Skills Development for Staff

New staff receive information on the school's acceptable use policy as part of their induction

All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community

All staff are encouraged to incorporate Online Safety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

Managing the School Online Safety Messages

We endeavour to embed Online Safety messages across the curriculum whenever the internet and/or related technologies are used

The children's Online Safety Acceptable Use Agreement - Staying Safe when using ICT and the Internet will be introduced to the pupils at the start of each school year

Online Safety rules will be prominently displayed in every classroom and around the school

The key Online Safety advice will be promoted widely through school displays, newsletters, class activities, the school website, assemblies and theatre companies

Equal Opportunities

Pupils with Additional Needs

The school endeavours to create a consistent message with parents/carers for all pupils and this in turn should aid establishment and future development of the schools' Online Safety rules.

However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of Online. Internet activities are planned and well managed for these children and young people.

Incident Reporting and Online Safety Incident Log

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Head of School or the Assistant Headteacher. The Data Protection Officer (DPO) must be notified of any security breaches, loss/corruption of or unapproved access to personal information.

Online Safety Incident Log

An incident log is kept to record and monitor what is happening. This is analysed to identify trends or specific concerns. This is recorded on CPOMS.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting Online both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss Online with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website and Twitter)

The school disseminates information to parents relating to online Safety where appropriate in the form of;

- Online Safety information meetings
- Posters
- School website information
- Newsletter items
- Invites to watch Online Safety performances with their children

Social Media, Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important

part of our daily lives.

- Our school uses Twitter to communicate with parents and carers. Mrs Mitchell (Executive Head Teacher) and Mrs Robinson (Head of School) are responsible for all postings on these technologies and monitor responses from others
- When parents take photographs and video of children when they are part of a performance or event at school it is requested that they are not to post on social media sites
- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law

E-Mail

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or

international. We recognise that pupils need to understand how to style an email in relation to their age and how to behave responsibly online.

Staff and governors should use their YHCLT Google Mail account for all official communication to ensure that children are protected through the traceability of all emails through the school email system. In addition, it is important that governors are protected against possible allegations of inappropriate contact with children. This is to help mitigate the chance of issues occurring and is an essential element of the safeguarding agenda.

Managing email

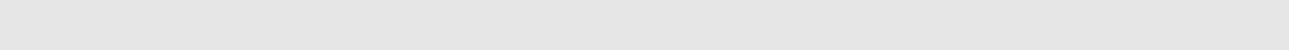
- The YHCLT gives all staff their own email account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed
- Staff should use their YHCLT Google Mail for all professional communication.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. The YHCLT Google Mail account should be the account that is used for all school business
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses
- All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Staff sending emails to external organisations, parents or pupils are advised to cc. the Head of School or Assistant Headteacher
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- Emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.
- All pupil email users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission, virus checking attachments
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting email
- Staff must inform the school IT support team
- Pupils are introduced to email as part of the Computing Programme of Study
- However staff access the YHCLT Google Mail (whether directly, through google

when away from the office or on non-school hardware) all the school email policies apply

Sending emails

- Use your own YHCLT Google Mail account so that you are clearly identified as the originator of a message
- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- YHCLT Google Mail is not to be used for personal advertising

Receiving emails

- Check your email regularly
 - Activate your 'out-of-office' notification when away for extended periods
 - Never open attachments from an untrusted source; consult your network manager first
 - Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
 - The automatic forwarding and deletion of emails is not allowed
- 

Internet Access

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

All internet activity is logged by the school's internet filtering system (Smoothwall). These logs may be monitored by YHCLT IT Support upon the request of the Head of School. Whenever any inappropriate use is detected it will be followed up, investigated and actioned by the Head of School.

Managing the Internet

The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity

Staff will preview any recommended sites, software and apps before use

Searching for images through open search engines is discouraged when working with pupils

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.

All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources

All users must observe copyright of materials from electronic resources

Radicalisation Procedures and monitoring

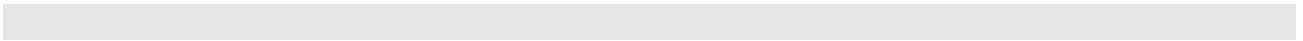
Serious incidents involving radicalisation have not occurred at Oldfleet Primary School to date, however, it is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we teach. Staff are reminded to suspend any professional disbelief that instances of radicalization 'could not happen here' and to refer any concerns through the appropriate channels (currently via the Designated Safeguarding Lead – Alyson Thompson). Regular monitoring and filtering is in place to ensure that access to inappropriate material on the internet and key word reporting is in place to ensure safety for all staff and students.

Computer Viruses

- All files downloaded from the Internet, received via email or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on school ICT equipment.
- If your machine is not routinely connected to the school network, you must make

provision for regular virus updates through YHCLT IT Support.

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.



Data Security

The accessing and appropriate use of school data is taken very seriously.

Security

- The school gives relevant staff access to its Management Information System SIMS , with a unique username and password
 - It is the responsibility of everyone to keep passwords secure
 - Staff are aware of their responsibility when accessing school data in line with GDPR
 - Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
 - Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
 - Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
 - We do not permit the use of memory sticks or other removable storage devices that is not password protected
-

Remote Access

You are responsible for all activity via your remote access facility

Only use equipment with an appropriate level of security for remote access

To prevent unauthorised access to school systems, keep all dial-up access information such as logon IDs and Passwords confidential and do not disclose them to anyone

Select Passwords to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers

Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is

Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment

Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

Policy breaches may also lead to criminal or civil proceedings.

The General Data Protection Regulation (GDPR) came into force on May 25th 2018. The Information Commissioner's Office can serve organisations with fines up to 20 million Euros depending on the severity of the breach.

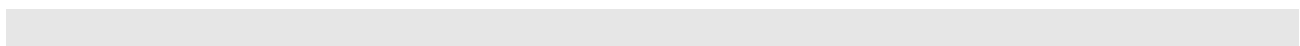
The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice, Report to Parliament on data protection issues of concern

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are as follows: Pauline Robinson (Head of School) and Vicky Mounsor (Assistant Head Teacher and DSL)

Please refer to the relevant section on Incident Reporting Online Safety.



Current Legislation

Acts Relating to Monitoring of Staff email

General Data Protection Act (GDPR)

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

<http://www.legislation.gov.uk/ukpga/2018/12/contents>

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

<http://www.hms0.gov.uk/si/si2000/20002699.htm>

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

<http://www.hms0.gov.uk/acts/acts2000/20000023.htm>

Human Rights Act 1998

<http://www.hms0.gov.uk/acts/acts1998/19980042.htm>

Other Acts Relating to Online Safety

Racial and Religious Hatred Act 2006

It is a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of “*Children & Families: Safer from Sexual*

Crime” document as part of their child protection packs.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual’s motivation, the Act makes it a criminal offence to gain:

access to computer files or software without permission (for example using another person’s password to access files)

unauthorised access, as above, in order to commit a further criminal act (such as fraud)

impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone’s work without obtaining their author’s permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else’s material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

General Data Protection Regulation (GDPR)

<http://www.legislation.gov.uk/ukpga/2018/12/contents>

The Freedom of Information Act 2000

<https://ico.org.uk/for-organisations/guide-to-freedom-of-information/>

Counter-Terrorism and Security Act 2015 (Prevent), Anti-Radicalisation & Counter-Extremism Guidance

<https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrens-services>

The E-Safety Policy should be read in conjunction with the following Safeguarding policies

- Child Protection Policy
- Behaviour Policy
- Anti Bullying Policy
- Data Protection Policy
- Whistle Blowing Policy
- Computing Curriculum Policy

Date : Autumn 2020

Review : Autumn 2021