Children and learning at the heart of our CARE-ing community	**Old Fletton Primary School** **Online Safety & Internet Acceptable Use Policy** Version 10 - March 2024

OUR ASPIRATION FOR OLD FLETTON PRIMARY SCHOOL	
Online safety	We aspire for all our pupils to feel secure in their abilities to use technology and the internet in their learning development and feel confident and safe in doing so.
Internet use	Recognising the learning opportunities available and ensuring that online activities are appropriately carried out using Old Fletton Primary School's Internet Rules.
Linked policies	Acceptable Use of Mobile Technology Code of Conduct Whistleblowing Policy Behaviour & Expectations Policy Child Protection & Safeguarding Policy

What is the policy for?	This policy is for all members of the Old Fletton Primary School community to ensure a common understanding about our expectations on the safe use of the internet.
Who has devised and contributed to this policy?	This was initially devised as the Internet Security Policy by the Deputy Headteacher and ratified by Governors. Subsequently this has been reviewed and amended by the Headteacher and ICT subject champion.
How will this policy be communicated?	This policy is available on the school website and in the Headteacher's office.
How will this policy be monitored?	The policy will be reviewed every year in line with the policy monitoring schedule.

At Old Fletton Primary School internet access is available to all staff on school laptops and iPads. It is also available to all pupils on school laptops and iPads as part of our curriculum provision. Personal devices must not be connected to the school wi-fi service.

Staff at Old Fletton Primary School strongly believe in the educational value of online services and recognises their potential to support the curriculum. Every effort will be made to provide quality experiences using this information service, however, inappropriate and/or illegal interaction with any information service is strictly prohibited.

Listed below are the provisions of this policy. If any member of staff violates these provisions, access to the internet will be denied and the member of staff may be subject to disciplinary action. If any pupil breaks the Pupil Internet Rules they may have their access withdrawn.

Staff

Personal Responsibility

As a representative of the school, every staff member will accept personal responsibility for reporting any misuse of the network to the Deputy Headteacher or Headteacher. Misuse may come in many forms, but it is commonly viewed as any message(s) sent or received that indicate or suggest pornography, unethical or illegal requests, racism, sexism, inappropriate language or images, any use which may be likely to cause offence and other issues described below.

Acceptable Use

The use of the internet will be in support of education and research in accordance with the educational goals and objectives of Old Fletton Primary School however, occasional personal use is acceptable and may be subject to monitoring. Every staff member is personally responsible for this provision at all times when using the internet.

Email

Staff members must use their school email address to conduct any school business and/or communications and not personal email addresses.

Online behaviour and Privacy

Staff are expected to abide by the generally accepted rules of online behaviour. These rules include, but are not limited to the following:

- Be polite and never send or encourage others to send abusive messages.
- Use appropriate language remembering that you are a representative of the school on a global public system. You may be alone with your computer, but what you say and do can be viewed by others. Never swear, use vulgarities or any other inappropriate language. Illegal activities of any kind are strictly forbidden, including posting inappropriate images.
- Privacy - do not reveal any personal information to anyone, especially the home address or personal telephone of yourself or any other staff members or pupils.
- Do not reveal your password to anyone. If you think someone has obtained your password, contact the Deputy Headteacher immediately.
- Email is not guaranteed to be private and messages relating to, or in support of, illegal activities may be reported to the authorities.
- Do not use the internet in any way that would disrupt use of the services by others.
- Pupil laptops/electronic devices/work must only be accessed by staff for the purposes of supervising and supporting children's learning.
- Respect the rights and beliefs of others.

Services

Old Fletton Primary School makes no warranties of any kind whether expressed or implied, for the internet service it is providing. Old Fletton Primary School will not be responsible for any damages suffered whilst on this system. These damages include loss of data as a result of delays, non-deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, or your errors or omissions. Use of any information obtained via the internet or other information systems is at your own risk. Old Fletton Primary School specifically denies any responsibility for the accuracy of information obtained via its Internet services.

Security

Security on any computer system is a high priority because there are so many users. If you identify a security problem, notify the Deputy Headteacher at once. Never demonstrate the problem to another person. All use of the system must be under your own username and password unless specifically directed. Remember to keep your password to yourself. Anyone caught disclosing passwords may have their access denied and may be subject to disciplinary action. Any user identified as a security risk may be denied access to the system and be subject to disciplinary action.

Vandalism

Vandalism is defined as any malicious attempt to harm or destroy any equipment or data of another user or of any other networks that are connected to the system. This includes, but is not limited to, the uploading or creation of computer viruses, the wilful damage of computer hardware, whether connected to the network or not, the deletion of data from its place of storage.

Social Media

Staff at Old Fletton Primary School must not use social media services via the school internet unless it is a school social media account, e.g. Twitter. Social media sites are a minefield of potential breeches of personal information etc. If a member of staff uses these sites at home then they have a professional responsibility to ensure security settings are at the highest level so that their content does not bring their professionalism into question. If school is made aware of any misuse of social media services outside school by any stakeholder it will advise relevant parties to contact the provider/police.

Data Protection

All staff have encrypted hard drives.

Pupils

All pupils at Old Fletton Primary School will understand that using the internet is a valuable tool for their learning and will follow these class rules:

- ☑ I will use the internet to support and enhance my learning
- ☑ I will only visit websites I have been told to
- ☑ I will not use You Tube at any time, although my teacher may show me a clip if it supports my learning
- ☑ I will not go on any games during reward times without seeking the permission from the adult in the room
- ☑ I will not use social media sites
- ☑ If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately
- ☑ I know the school may check the computer I have used and may monitor the websites I visit.
- ☑ I understand that if I break these rules on purpose, I could be stopped from using the internet, or computers.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website and on-line pupil records

Policy Statements

Education – Students / Pupils

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 / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the pupil Internet Rules and be encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- 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, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that E2BN temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents/Carers

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 / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g. swgfl.org.uk / www.saferinternet.org.uk / www.childnet.com/parents-and-carers

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The internet access is filtered for all users through E2BN Protex and searches are monitored by the Designated Safeguarding Lead.