Yewstock School

E-Safety Policy

Date reviewed by CC	**15.11.2021**	**Policy Type**	**School**
Date adopted by FGB	**29.11.2021**	**Review Cycle**	**Annually**
Date of next Review	**14.11.2022**	**Signed by Chair of Governors**	
			

Yewstock School

E-Safety Policy

Rationale

At Yewstock School we take E-Safety very seriously and see it as our duty to keep our pupils safe whilst using technology not only in school but also at home. New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times. Staff should always seek to inform and communicate any apps/games/trends on social media that they come across as a concern or are warned about, to parents so students can remain safe in and out of school.

The policy covers 3 main areas; children's safety, staff's responsibilities and support for parents.

E-Safety Committee

An E-Safety Committee has been set up which includes, the ICT Subject Leader, a nominated Governor, the IT Systems Manager, and a member of the Leadership and Management Team.

The group's responsibility is to annually review the E-Safety policy and curriculum. The group meets twice yearly. Minutes are taken which are available in the E-Safety folder in the Staff Resources drive. A hard copy is located in the E-Safety folder.

Network Safety

The school's Network is presently managed by Jamie Dawe the ICT Systems Technician who works with the DSL and is responsible for the safety of the Network and the pupils / staff who access it.

A termly meeting takes place with representatives of the E-Safety Committee. During this meeting any issues with the Network and E-Safety issues are dealt with.

Senso.Cloud, a monitoring system which identifies safeguarding concerns, is checked by Jamie Dawe and the DSL. Issues that are highlighted in these checks are written in the online safeguarding reporting system 'MyConcern' and are then dealt with by the Leadership and Management Team.

Safety and Responsibilities for Staff

All staff are required to read and sign an Acceptable Use Agreement (AUA) which clearly states the responsibilities of staff using technology in the work place.

This will be signed when they commence their employment at Yewstock School and will be reinforced each year during the staff's E-Safety update.

The AUA lists the responsibilities of all staff and covers the use of digital technologies in school: i.e. E-mail, Internet, Intranet and network resources, and this will also apply to 'Bring Your Own Device' if it is adopted in the future.

Staff Code of Conduct

All staff and visiting professionals are required to agree to the Acceptable Use Agreement:

Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will educate the pupils in my care in the safe use of ICT and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems and digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, iPads etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the Designated Safeguarding Leads and ICT Systems Technician.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify pupils names or other personal information.
- I will only use chat and social networking sites in school in relation to school business.
- I will only communicate with pupils and parents and carers using official school systems. Any such communication will be professional in tone and manner.
- I understand that using my personal email addresses / mobile phone / social networking sites for such communications in not allowed, to protect me from abuse.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

Yewstock School and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (PDAs / iPads / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up.
- I will not upload, download or access any materials which are illegal (e.g. child sexual abuse images, racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless I have checked whether it is alright to do so with the ICT systems Technician.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I will be aware that discussing issues related to school on a social media forum may potentially bring the school into disrepute.

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors or the Local Authority and in the event of illegal activities the involvement of the police.

I understand that my actions will leave a digital footprint, therefore understand clearly that any negative comments/un-professional/controversial statements are my responsibility.

E-Safety training will be provided to all members of staff once a year and it is each person's responsibility to attend this session. These sessions will be arranged by the ICT Coordinator.

It is very important that staff make sure that the pupils they are responsible for are using the Internet safely. High risk students will be highlighted by the Leadership and Management Team and staff will be made aware of these students.

Safety and responsibility for Pupils

Although some of our pupils are unable to access the Internet we have a good percentage of pupils who are able to use the Internet independently and therefore are at risk from either deliberately accessing inappropriate material or, due to their level of literacy, accidently accessing harmful sites.

No child is able to access the Internet in school without their parents giving permission to do so. This consent form is filled in when the child starts school and is kept on record until they leave; it will only need amending if a parent/carer would like to change it.

All pupils who are able will have to sign an AUA and this will be completed every yeaR. This document will clearly state their responsibilities when using technology in school.

All pupils will receive E-Safety training. They will also have the opportunity to be reminded regularly of E-Safety by all Teachers and Teaching Assistants. Students will receive regular termly help guides and parent awareness information on potential and concurrent threats. Students will receive a termly e-safety focus

from younger years to older years to ensure scaffolding and reinforcement of basic and evolving whole school e-safety ethos.

All pupils will be taught how to use all technologies in a responsible and safe way. This will be part of the ICT curriculum.

No child may appear on the Web Site without their parent/carers consent, the consent form is completed when the child starts school and is kept on record until they leave; it will only need amending if the parent/carer would like to change it.

Support for Parents

As a school we believe it is our duty to support parent and carers in keeping their child safe while using technology within the home environment. Computers and other devices in the home are more open and don't have the security features which we have in school, which does make the child more vulnerable in this environment.

The school web site will have information regarding E-Safety for parents / carers and young people in order to reach the widest audience possible.

An E-Safety link is kept up-to-date on the school website with advice and resources for parents to use.

Parents receive a termly newsletter specifically structured around a breakdown of national online safety threats and possible areas of concern, together with this they also receive an e-safety pack of key parent guides that are tailored around threats that have been raised and subject areas relevant at that time.

This policy should be read in conjunction with the Single Equality Policy. The general equality duty requires that, in the exercise of their functions, schools must have due regard to the need to eliminate unlawful discrimination, harassment, victimisation and other conduct prohibited by the Equality Act 2010. This school endeavours to advance equality of opportunity and foster good relations for all.