At Yealmpstone Farm Primary School we promote equality between all people, recognisingthe Equality Act 2010'

Online safety and Acceptable Use Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers and visitors) who have access to and are users of the school's ICT systems, both in and out of our setting.

Our staff are empowered, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of the school building, but is still linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for the e-safety of individuals and groups

Governors are responsible for the approval of the e-safety Policy and for reviewing the effectiveness of the policy. This policy reflects expectations of KCSiE 2024.

The Headteacher is responsible for ensuring that:

- The safety (including e-safety) of members within the school
- Relevant staff receive suitable training and development to enable them carry out their safety roles and to train other colleagues, as relevant
- Systems are in place to allow for the monitoring and support of those in the school who carry out the internal e-safety monitoring role. This is to provide a safety net and also to support those colleagues who take on important monitoring roles
- Provide information to the Governing Body as appropriate

Member of SLT with responsibility for e-safety

- Take day to day responsibility for e-safety issues and oversee the sanctions for breaches of rules relating to e-safety

- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provide training and advice to staff
- Liaise with the Local Authority Designated Officer (LADO) or Police as appropriate
- Liaise with external partners as appropriate

Technical Staff

- Ensure that the school's infrastructure is secure and is not open to misuse or malicious attack and that all aspects of the school's ICT systems are secure, in line with the school's guidance and policies.

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of current school e-safety policy and practices
- They have read and understood the appropriate ICT agreements
- They report any suspected misuse or problem to a member of SLT
- Digital communications with pupils are only on a professional level and carried out using official school systems
- It is understood that social media can play an important part in communication between the school and pupils, parents/carers; however, there is also a need to ensure it is used in an appropriate and safe way.
- Before any member of staff sets up a resource such as a student blog space, they must seek permission from the Headteacher and they should ensure that appropriate steps are taken to make such social media 'private' so that only people they approve can access it. The member of staff will then be responsible for the posts made on the site and for moderating the content from other users/contributors
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Pupils understand and follow the school's e-safety and Acceptable Use Policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current best practice with regard to these devices
- In lessons where internet use is pre-planned, pupils should be guided to sites that are checked as suitable for their use and that processes are in place to deal with any unsuitable material that is found in internet searches.

Designated Safe-guarding Person (and Deputy) are trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Children (appropriate to age / stage of pupil)

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand the Trust's policies on the taking/use of images and on cyber-bullying
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions outside of the school gates, if related to their membership of the school.

Parents

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through communications and the website.

Parents and carers will be responsible for:

- Endorsing the school policy
- Accessing the school website in accordance with the relevant Acceptable Use Policy.

Education and Training

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of the ICT programme of study
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and within the PSHE curriculum
- Pupils will be taught whenever an opportunity occurs to be critically aware of the material/content they access on-line and be guided to validate the accuracy of information
- Pupils will be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside the school
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff will act as good role models in their use of ICT, the internet and mobile devices.

Education and Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

Training will be offered as follows:

- E-safety training for all staff is included as part of Level 1 & 2 child safeguarding training
- All new staff will receive e-safety training as part of their induction programme, ensuring they understand the E-safety Policy and Acceptable Use Policy.

Training – Governors

- The school's online child safeguarding training covers the relevant elements of safety training. Governors are required to undertake the school's online training on their appointment.

Infrastructure, equipment, filtering and monitoring

The school will be responsible for ensuring that the infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- All users will have clearly defined access rights to school's ICT systems
- All users will be provided with a username and password. Users will be required to change their password regularly
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- In the event of the filtering system needing to be switch off for any reason, or for any user, this must be logged and carried out by a process that is agreed by Headteacher
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager who resides in the LA.
- A system is in place for users to report any actual / potential safety incident to SLT: these must be logged on CPOMs.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school's systems and data
- Personal use of the school's ICT systems should be limited to what may be deemed reasonable. The services are provided predominantly for education purposes
- Neither staff nor pupils should install programmes or other software on workstations, portable devices or servers, without the prior express, written permission of the school's Network Manager
- The school's ICT infrastructure and individual workstations are protected by up-to-date virussoftware
- Personal data (as defined by the Data Protection Act) cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured by password or other means

- Where staff have email accounts and other data on their phone or other mobile device they must ensure that the device is locked with a password.

Curriculum

- E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.
- 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, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit
- 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

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- 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
- Staff are allowed to take digital / 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 taken on school equipment; the personal equipment of staff should not be used for such purposes. They should also only be stored on the school's network and not on any personal device
- 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
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Written permission from parents will be obtained before photographs of pupils are published on the school website (this is covered as part of the agreement signed by parents or carers)

- Be aware that downloading, copying or printing images from the internet may also breach copyright laws.

Data Protection

Personal data (as defined by the Data Protection Act) will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss ormisuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data
- Transfer data using encryption/ secure password protected devices or ensure that the file is password protected.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected, if this is the case then each individual file will need to be password protected)
- the data must be securely deleted from the device, once it is no longer required.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

- Users need to be aware that email or other online communications may be monitored
- Users must immediately report, to a member of SLT, the receipt of any email or online communication that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and pupils or parents / carers (email, Dojo message etc.) must be professional in tone and content. These communications should only take place on official (monitored) school systems.
- Pupils should be taught about email/online safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails or online

messages and be reminded of the need to write messages clearly and correctly and not include any unsuitable or abusive material.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is obviously be banned from the school ICT systems. Other activities e.g. Cyber-bullying, use of electronic communications to radicalise children or others, is banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

Responding to incidents of misuse

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. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials
- radicalisation of others

The Headteacher must be informed immediately.

The Headteacher and any other relevant members of the SLT must inform the relevant authorities immediately of any concerns/ infringements.

Appendix 1

Yealmpstone Farm Primary School

Acceptable use agreement for parents and pupils
Network access and use of graphic image

Please complete and return this form to the class teacher.

Pupil:
I have read and understand the school Rules for responsible **ICT** use, and agree to use them. I will work with **online activities**, e-mail and other devices linked to our learning at school in a safe and responsible way and promise to keep to all the restrictions explained to me by school. I agree to give any devices to my teacher for the day if they ask.

Pupil's name _____ Pupil's signature _____

Parent:

I have read and understand the school Rules for responsible **ICT** Use, and as the parent or legal guardian of the pupil signing above, I agree that my son or daughter should use the **Internet**, e-mail and other **ICT** facilities as part of their studies at school. I understand that the school will take reasonable precautions to ensure that pupils can not access inappropriate materials, including the teaching of **Internet** safety skills to pupils, but accept that ultimately the school can not be held responsible for the nature and content of materials accessed through the **Internet**. I accept responsibility for setting and conveying standards for my son or daughter to follow when selecting, sharing and exploring information and media, and acknowledge that they will be deemed to be accountable for their own actions.

Parent's signature _____Date: ___/___/____

Pupil's name _____

class teacher / year group_____

Home Telephone _____

Mobile Telephone _____

Email address _____

Use of Images

From time to time, we would like to celebrate children's achievements and publicise them on the school website and use our twitter/dojo/website feeds to acknowledge good practice in school. This may mean using photographs and video images.

I **give** permission for the image / moving image of the child named above in the school website/dojo and our monitored twitter feeds.

I **give** permission for the image of the child named above to be used in promotional activities initiated and vetted by the senior staff in school.

PLEASE WRITE THE WORDS **DO NOT** IN THE SPACE PROVIDED IF YOU WANT YOUR CHILD'S IMAGE TO BE **EXCLUDED** FROM THESE CELEBRATIONS.

This document is updated and renewed on an annual basis. Parents **should keep this information** for future reference and **return the separate permission page** for school files.

General Information

We will allow pupils, teachers, other employees and the community access to the school's computers, network services, and the Internet feed. All pupil activity, when using the network and connected data services in school, must be in support of education and/or research and must be appropriate to the educational objectives of the school. Pupils who access the Internet from the school site are responsible for everything that takes place on their computers and all Internet activity is monitored.

Benefits

Access to google apps and related learning resources will enable staff and pupils to:

- Explore many databases and other sources of information
- Engage in communication with other educational users around the world
- Be included in Government initiatives and global educational projects
- Find news and current events in relation to their learning objectives
- Take part in live discussion with experts
- Publish and display work by using agreed means (i.e. web site, twitter feeds and google apps sharing)
- Make use of content from subscribed providers and southwest grid for learning SWGfL.

Effective Use

Internet access will be planned to enrich and extend learning activities as an integral aspect of the curriculum.

Pupils will:

- *Be given clear objectives for Internet use*
- *Be educated in responsible use and given necessary e-safety information*
- *Be supervised appropriately*
- *Learn to search for and discriminate between valid and inappropriate material*
- *Learn to copy, save and use material found on the Internet without infringing copyright*

E Safety

Internet access at our school is effectively filtered by the Southwest Grid for Learning (SWGfL), our Internet Service Provider (ISP); every effort is made to prevent unsuitable material from being accessed. Ultimately parents and guardians of minors are responsible for setting the standards that their children should follow when using media and information sources.

Personal Security Guidelines

Pupils should

- Never reveal personal information and passwords, either their own or others, including home addresses, telephone numbers and personal Email addresses
- Not use photographs of themselves on any online source unless permission by appointed members of staff has been given
- Never meet people in person that they have contacted on the Internet without permission by appointed members of staff

- Notify their teacher whenever they come across information or messages that they consider to be dangerous, inappropriate, or make them feel uncomfortable
- Be aware that the author of an Email or Web page may not be the person they claim to be

Managing Email

Email addresses of pupils are not advertised publicly. Children may receive Email directly from known addresses and they may also use their personal Email address when replying to known recipients.

Email may contain attached documents and files. These could potentially carry viruses. Users are requested to ensure that a virus-checking programme and an effective firewall are loaded before opening any Email attachments.

Access Permission

Pupils are responsible for appropriate behaviour on the school's computer network just as they are in the classroom or on the school playground. Communications on the network are often public in nature. General school rules and our Behaviour Policy apply and it is expected that users will comply with the guidelines of this policy. Pupils are personally responsible for their actions when using school equipment to access computer resources outside the school network.

Parental Support

Pupils could potentially have unfiltered, unsupervised Internet access at home. All parents should be aware of the concerns and benefits of Internet use. Parents are therefore encouraged to come in to school to work alongside the teacher to experience online content used first hand and to help in the supervision of the children. General information of Internet safety can be found in the parent zone of the school website. www.yfps.net

Acceptable use and Guidelines

Privacy
Teachers and staff may review documents and log files to ensure that pupils are using the system responsibly.

Software
Pupils should never download, load or install any software, shareware, or freeware, or load any such software from memory sticks, unless they have permission from their teacher. Pupils may not copy other people's work or intrude into other people's files without permission.

Inappropriate materials or language
Profane, abusive or impolite language should not be used to communicate through google apps or Internet messaging, nor should materials be accessed which are not in line with the rules of school behaviour. A good rule to follow is never view, send, or access materials that you would not want your teachers or parents to see. Should pupils encounter such material, they should immediately report it to a member of staff.

Home School Links
All home school links through the web site portals are offered on a goodwill basis. All content should only be used in connection with school related matters. The same rules and restrictions apply when using network resources from outside the school building. All access should be appropriately supervised and any misuse should be reported to a member of staff.

Social Networking
Many children are increasingly using social networking sites at home. Every effort should be made to monitor all activity on such sites and use of these sites in school is restricted. This is a constantly developing aspect of using internet enabled devices and must be monitored by a member of staff if any pupil requires access.

Internet enabled devices
Children should not access the internet using a personal wireless device such as netbook, mobile phone or media / music device unless it is part of a planned activity or they have separate permission EVERY time they use it.

The Law
Pupils should never knowingly use the computers to engage in activities that may be in violation of the law.