Yarrells School & Nursery

E-SAFETY POLICY

Policy Lead (Position (and Initials)): **Head of Computing & E-Safety Champion (RSE)**
Date of Last Review: **May 2021**
Date of Next Review: **May 2022**

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 and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times.

The requirement to ensure that children and young people are able to use the Internet and related communication technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside school.

This policy is concerned with Yarrells School's approach to e-safety. This policy is to be implemented by:

- All staff
- Volunteers

This policy is addressed to:

- All staff
- Volunteers
- Pupils
- Parents
- Visitors (where applicable)

The purpose of this policy is to highlight the need to educate children and young people about the benefits and risks of using new technology, and to provide safeguards and awareness for users to enable them to control their online experiences. This e-safety policy should be used in conjunction with other school policies (e.g. behaviour, anti-bullying and safeguarding policies).

E-safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology.

The school has a designated e-safety champion, who is responsible for this policy and any further updates.

Contents

1. Why is Internet use important?
2. How does Internet use benefit education and enhance learning?
3. Good habits and dangers to consider
4. Authorised Internet access
5. World Wide Web
6. Email
7. Social networking
8. Filtering
9. Managing emerging technologies
10. Published content and the school website
11. Publishing pupil's images and work
12. Information system security
13. Protecting personal data
14. Assessing risks
15. Handing e-safety complaints
16. Responsibilities and powers
17. Communication of the policy

1. Why is Internet use important?

1.1. The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

1.2. Internet use is part of the National Curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.

1.3. Many pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

2. How does Internet use benefit education and enhance learning?

2.1. Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries
- educational and cultural exchanges between pupils world-wide
- access to experts in many fields for pupils and staff
- professional development for staff through access to national developments, educational materials and effective curriculum practice
- collaboration across support services and professional associations
- improved access to technical support including remote management of Networks and automatic system updates
- exchange of curriculum and administration data with the Local Authority and DCSF
- access to learning wherever and whenever convenient

2.2. The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.

2.3. Pupils will be taught what Internet use is acceptable and what is not, and given clear objectives for Internet use.

2.4. Internet access will be planned to enrich and extend learning activities.

2.5. Staff should guide pupils to online activities that will support learning outcomes planned for the pupils' age and maturity.

2.6. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2.7. See Appendix 1: Pupil Acceptable Use Policy Agreement for a description of acceptable and unacceptable computer use rules.

3. Good habits and dangers to consider

3.1. Good habits – e-safety depends on effective practice at a number of levels:

- responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies
- sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use
- safe and secure broadband from the provider including the effective management of content filtering
- Advice and guidance from National Education Network standards and specifications
- Content filtering is carried out in-house by the e-safety champion and is therefore current and quick to update if necessary

3.2. Dangers to consider – some of the dangers users may face include:

- access to illegal, harmful or inappropriate images or other content
- unauthorised access to / loss of / sharing of personal information
- the risk of being subject to grooming by those with whom they make contact on the Internet
- the sharing / distribution of personal images without an individual's consent or knowledge
- inappropriate communication / contact with others, including strangers
- cyber-bullying
- access to unsuitable video / Internet games
- an inability to evaluate the quality, accuracy and relevance of information on the Internet
- plagiarism and copyright infringement
- illegal downloading of music or video files
- radicalisation
- the potential for excessive use which may impact on the social and emotional development and learning of the young person.

3.3. As with all other risks, it is impossible to eliminate those dangers completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

3.4. Regular training and awareness will take place in classes for pupils along with Parent Meet sessions on E-Safety and INSET sessions for staff.

4. Authorised Internet access

4.1. All staff must read and sign Appendix 3: Acceptable Use for Staff and Volunteers before using any school ICT resource and serves as a part of the induction paperwork for all employees and volunteers.

4.2. Parents will be informed that pupils will be provided with supervised Internet access. Parents will be asked to sign and return Appendix 2: Parental Acceptable Use Policy Agreement.

4.3. Pupils will be asked to sign and return Appendix 1: Pupil Acceptable Use Policy Agreement

5. World Wide Web

5.1. If staff or pupils discover unsuitable sites, the URL (address), time and content must be reported to the e-safety champion who will investigate and take appropriate action, liaising with the broadband provider if necessary.

5.2. The school will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.

5.3. Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

6. Email

6.1. Pupils may only use approved e-mail accounts on the school system.

6.2. Pupils must immediately tell a teacher if they receive offensive messages.

6.3. Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

6.4. Pupils may not access others pupil's accounts.

6.5. Access in school to external personal e-mail accounts may be blocked.

6.6. E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

6.7. The forwarding of chain letters is not permitted.

7. Social networking

7.1. Schools should block/filter access to social networking sites and newsgroups unless a specific use is approved.

7.2. Pupils will be advised never to give out personal details of any kind which may identify them or their location.

7.3. Pupils should be advised not to place personal photos on any social network space.

7.4. Pupils should be advised on security and encouraged to set passwords where appropriate, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

7.5. Pupils and parents should be made aware that some social networks are not appropriate for children of school age.

8. Cyber-bullying, Exploitation & Extremism

8.1. Cyber-bullying like all forms of discrimination is not tolerated at Yarrells. Pupils are encouraged to report cyber bullying to teachers or the Senior Leadership Team.

8.2. The school promotes positive online communication, counteracting cyber-bullying in all forms; dealing with incidents reported or detected.

8.3. The school promotes safe communication online, to counteract exploitation and extremism, through well-established systems for monitoring, developing of pupils understanding and reporting of concerns with relevant authorities (In line with the revised Prevent Duty Guidance in England and Wales, 2015).

8.4. The school will work in partnership with the external IT and broadband provider, Schoolcare, to ensure filtering systems are as effective as possible. The filtering system is actively monitored by Schoolcare and any issues that arise regarding inappropriate content getting through the filter are dealt with quickly and effectively. Any issues can be reported immediately to Schoolcare by the school and are usually resolved within a few hours.

8.5. The actual policy sets (what categories are allowed/disallowed for certain users, what keywords are allowed/disallowed, monitoring of reports, etc.) are maintained in partnership with Schoolcare and frequently checked during their monthly visits.

9. Managing emerging technologies

9.1. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. This includes mobile phones, smart watches and any similar devices.

9.2. Mobile phones and other smart devices are not allowed in school. If a mobile phone or other smart device is brought in to school it will be kept in the school office until the end of the day.

10. Published content and the school website

10.1. The contact details on the website should be the school address, e-mail and telephone number.

10.2. Staff or pupils' personal information will not be published.

10.3. The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

11. Publishing pupils' images and work

11.1. Photographs that include pupils will be selected carefully and will comply with the school's photography policy on the use of such images.

11.2. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or used on Social Media. See Appendix 2: Parental Acceptable Use Policy Agreement

11.3. Work can only be published with the permission of the pupil and parents.

11.4. Staff will use only school equipment to take photographs of pupils. Staff will ensure that the safe and appropriate use and storage of the equipment and memory cards containing any images of pupils is maintained. All images are to be stored securely on the school system as soon as possible from the time of use and deleted from the equipment and memory cards before the next use.

11.5. The use of personal devices (e.g. mobile phones, cameras) to take images of pupils is strictly forbidden.

12. Information system security

12.1. School ICT systems capacity and security will be reviewed regularly.

12.2. Virus protection will be installed and updated regularly.

12.3. Security strategies will be discussed with our technical support team and broadband provider if necessary.

12.4. Staff passwords must be kept secret, and can be changed if necessary to prevent unauthorised access.

13. Protecting personal data

13.1. The Data Protection Act is relevant to e-safety since it impacts on the way in which personal information should be secured on school networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. This states that any data involving personal information about the school population (pupils, parents, staff and external agencies) must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Kept no longer than is necessary on secure school devices and servers that require a username and password;
- Processed in accordance with the data subject's rights;
- Secure;
- Only transferred to others with adequate protection.

13.2 In addition to this, personal emails must not be used for school business and all personal and sensitive information must only be sent by email when on a secure network. Secure accounts will need to be logged off after use to prevent unauthorised access.

14. Assessing risks

14.1. The school will take all reasonable precautions to prevent access to inappropriate material.

14.2. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

14.3. The school will audit ICT use routinely to establish if the e-safety policy remains adequate and that the ongoing implementation of the e-safety policy is appropriate. See Appendix 4: E-safety audit

15. Handling e-safety complaints

15.1. Complaints of Internet misuse will be dealt with by a senior member of staff.

15.2. Any complaint about staff misuse must be referred to the Headteacher.

15.3. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

15.4. Pupils and parents will be informed of the complaints procedure.

16. Responsibilities and Powers

16.1. The Education and Inspections Act 2006 empowers the Head, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and it empowers members of staff 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 school, but are linked to membership of the school.

16.2. The school will deal with such incidents within this policy, as well as associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of School.

16.3. The Head and Proprietors are responsible for ensuring the safety (including e-safety) of members of the school community, although the day-to-day responsibility for e-safety is be delegated to the Head of Computing who is also the E-Safety Champion, who is also supported by the Senior Designated Person for Safeguarding Children**.**

17. Communication of the policy

17.1. Pupils

17.1.1. Pupils will be reminded of the Rules for Internet access, as detailed in Appendix 1.

17.1.2. Pupils will be informed that Internet use will be monitored.

17.1.3. Differentiated acceptable use and e-safety expectations will be displayed prominently in classrooms near stationary computers for pupil usage in a way that pupils can access.

17.2. Staff

17.2.1. All staff will be given the school e-safety policy and its importance will be explained.

17.2.2. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

17.3. Parents

17.3.1. Whole community engagement is paramount in ensuring that the safe use of technology is communicated to all. Parents need to play the pivotal role in educating their children about staying safe while using a variety of different technologies as the school cannot apply filters or secure IT access out of the school environment. Parents' attention will be drawn to the school e-safety policy in newsletters, the school brochure and on the school website.

Appendix 1: Acceptable ICT use agreement (pupils and parents)
The following letter will be sent to pupils and their parents.

Yarrells School & Nursery

PUPIL ACCEPTABLE USE POLICY AGREEMENT

In school we have access to the Internet. This is a powerful tool which opens up new opportunities for everyone and promotes effective learning. We at Yarrells School are aware that young people should have an entitlement to safe Internet access at all times. However, the school and parents have a duty of care to protect children and ensure that Internet use is responsible and safe. Pupils and parents are asked to read and sign the following document relating to the safety and well-being of all our pupils. Child protection is a matter that we take very seriously at Yarrells and we thank you for supporting us with this.

E-safety Rules

- The school owns the computer network and can set rules for its use
- It is a criminal offence to use a computer or network for a purpose not permitted by the school
- Irresponsible use may result in the loss of network or Internet access
- All network and Internet use must be appropriate to education
- Copyright and intellectual property rights must be respected
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers
- Anonymous messages and chain letters are not permitted
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging
- The school ICT systems may not be used for private purposes, unless the Headteacher has given specific permission
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

As a pupil at Yarrells, I have the right:

- To use computer equipment, including the Internet, to help with learning both in lessons and extra-curricular activities.

As a pupil at Yarrells, I have the responsibility:

- to always use ICT systems carefully so that no damage is caused to any of the hardware or programs

- to only use programs and web sites I have permission to use.
- to make sure I am safe when using ICT.
- to help others stay safe when using ICT.
- to respect others' work and not change anything unless I have permission.
- to be polite and courteous when communicating on-line, not using language that might be perceived as hurtful to others.
- to request permission from school staff before taking photographs or recording video content.
- to only use images that will not hurt or endanger anyone, respecting the wishes of any pupil, parent or staff member not to have their image(s) published online.
- not to attempt to bypass any of the school's filters as they are there to help me to stay safe online.

I will:

- be aware of "stranger danger", when I am working on-line.
- not tell or share personal information about myself or others (such as my full name, phone number or home address) when on-line.
- tell an adult immediately if I see anything unpleasant, not nice or that makes me feel uncomfortable.
- tell an adult if I get any messages from someone I don't know or that are unpleasant.
- not try to change any computer settings or programs.
- 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.
- immediately report any damage or faults involving equipment or software, however this may have happened.
- not post digital or video images of other children on the Internet or any social networking sites that are not directly associated with the school.

I understand:

- that if I break this agreement I will be warned, or possibly have my computer and internet access restricted while at school.
- that any work that is to be posted on the Internet must be checked by a member of school staff before it is shared online.
- that any illegal behaviour will be dealt with by the police.

Additionally, in the event that I am using any personal devices (smartphones, tablets etc) with permission 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 agree to my work, both written and digital, to be used for school materials such as the yearbook or promotional documents.

I have read and understand the above and I agree to do these things.

Name _____

Signed _____ Date _____

Appendix 2: Parental Acceptable Use Policy Agreement
To be sent home and returned with the Pupil Acceptable Use Policy Agreement

Yarrells School & Nursery

PARENTAL ACCEPTABLE USE POLICY AGREEMENT

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 effective learning. Young people should have an entitlement to safe Internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people are responsible and safe when using the Internet and other communications technologies for educational, personal and recreational purposes.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy Agreement is attached to this form so that parents and carers will be aware of the school expectations of the young people in their care. Please share the document with the pupil and sign as indicated. Parents are requested to sign this document to show their support of the school in this important aspect of the school's work.

- I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the Internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the Internet and using mobile technologies.
- I understand that my son's/daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
- If working on related material at home, I will encourage my child to adopt safe use of the Internet and digital technologies and will inform the school if I have concerns over my child's e-safety. I will ensure that he/she is supervised adequately when working on homework tasks.

The school strongly recommends that primary age children do not use social network sites such as Facebook, Instagram, 'Musical.ly' and Snapchat at home – as these sites carry an age-restriction and pose a risk to children.

Parent's consent for Internet access

I have read and understood the school e-safety rules and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but that the school cannot be held responsible for the content of materials accessed through the Internet.

I agree to my son/daughter's work, both written and digital, to be used for school materials such as the yearbook or other promotional documents.

Name _____

Signed _____ Date _____

Appendix 3: Acceptable Use for Staff and Volunteers

Yarrells School & Nursery

ACCEPTABLE USE FOR STAFF AND VOLUNTEERS

To ensure that all staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

This Acceptable Use Policy is intended to ensure that:

- Staff and volunteers are responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff are protected from potential risk in their use of ICT in their everyday work.

Yarrells Preparatory School will endeavour to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning. In return, Yarrells Preparatory School expects staff and volunteers to agree to be responsible users.

Acceptable Use Policy 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, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school can monitor my use of the ICT systems and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, etc) out of school and to my personal devices if used in school.
- I understand that the school ICT systems are intended for educational and administrative use only.
- 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 will immediately report any illegal, inappropriate or harmful material or incident that I become aware of, to the Head. In the case where the Head is the alleged perpetrator, I will report to the Director.
- I understand that safeguarding procedures must be followed if a child is considered to be at risk of harm.
- I will respect copyright and intellectual property rights.

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

- 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 (an up to date list of permissions can be gained from the school office). I will not use my personal equipment to record these images.
- I will communicate with pupils and parents/carers by email using the official school administration email address. I understand that staff members should not give a personal email address to communicate with parents in an official capacity.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programs.
- I will not upload, download or access any materials that are illegal (child sexual abuse images, criminally 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 programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not make large downloads or uploads that might take up Internet capacity and prevent other users from being able to carry out their work, unless I have permission.
- I will not disable or cause any damage to school equipment, or equipment belonging to others.
- I will only transport, hold, disclose or share personal information about others or myself in accordance with the school's personal data policies and 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, however this may have happened.

I understand that I am responsible for my actions in and out of school and I understand that this Acceptable Use Policy 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 out of school and my use of personal equipment in school or in situations related to my employment by the school.

I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action, in accordance with the school policy. This could include a warning, a suspension, referral to the Board of Directors and in the event of illegal activities, and the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines. I understand that this policy is to be read and implemented in conjunction with the E-Safety policy as well as other important policies such as Safeguarding.

I have read, understood and agree with the Acceptable Use for Staff and Volunteers Policy.

Name _____

Signed _____ Date _____

Appendix 4: E-safety audit

This quick self-audit will help the senior leadership team (SLT) assess whether the safety basics are in place:

Has the school an e-Safety Policy that complies with CYPD guidance?	
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
The Policy is available for parents:	
The E-Safety Champion is:	
Is E-Safety training provided for all staff and pupils?	
Do all staff sign an Acceptable Use Policy on appointment?	
Are the E-Safety rules for pupils displayed in all rooms with computers in?	
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access?	
Has the school filtering policy been approved by the SLT?	
Is personal data collected, stored and used according to the principles of the Data Protection Act?	