Wreningham VC Primary

Online Safety Policy

1 Corinthians 12:12, "There is one body but it has many parts. But all its many parts make up one body."

All policies at Wreningham VC Primary School should be taken as part of the overall strategy of the school and implemented within the context of our vision, aims and values as a Church of England School

Headteacher: Mr RP Jones
Chair Full Governing Body: Mr. Steve Kittle

Reviewed Summer Term 2024
Next Review Spring Term 2025
This policy was approved by the Governing Body 24/4/24**.**

Aims

Our school aims to:
● Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
● Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology.
● Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

1. Writing and reviewing the Online Safety policy

The Online Safety Policy relates to other policies including those for the curriculum, bullying and safeguarding.

● The school's Designated Safeguarding Lead (DSL) has overall responsibility for Online Safety. The DSL is supported by the subject lead who, alongside the ICT technician, monitors Online Safety across the school.
● Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been approved by governors.
● The Online Safety Policy and its implementation will be reviewed annually.
● Online Safety training is given to all staff on a regular annual basis. It was discussed by staff on Wednesday 17/4/24

2. Teaching and learning

Guidance:
https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools

2.1. Why Internet and digital communications are important

● The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.
● Internet use is a part of the curriculum and a necessary tool for staff and pupils.
● The school internet access is provided by Rydal and includes filtering appropriate to the age of pupils. The firewall is called Smoothwall and helps keep children safe and thriving in their digital lives.
● Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use. The school will teach pupils how to stay safe online by using the ICT code of conduct Think then Click rules.
● Pupils will be educated in the effective use of the internet.
● Pupils will be shown how to publish and present information appropriately to a wider audience.

2.2. Pupils will be taught how to evaluate internet content

●The school will seek to ensure the use of internet derived materials by staff and by pupils complies with copyright law.
● Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
● Pupils will be taught how to report unpleasant internet content e.g. reporting to a trusted straight away, as well as using the CEOP Report Abuse icon or Childline.

Pupils will be taught about online safety as part of the curriculum. The text below is taken from the National Curriculum computing programmes of study. It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education. All schools have to teach Relationships education and health education in primary schools.

<u>In Key Stage 1, pupils will be taught to:</u>

● Use technology safely and respectfully, keeping personal information private
● Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

<u>Pupils in Key Stage 2 will be taught to:</u>

● Use technology safely, respectfully and responsibly
● Recognise acceptable and unacceptable behaviour
● Identify a range of ways to report concerns about content and contact

2.3 By the end of primary school, pupils will know:

● That people sometimes behave differently online, including by pretending to be someone they are not
● That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
● The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
● How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
● How information and data is shared and used online.
● What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
● How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

The parents' page of the school website provides links designed to signpost parents and children to the CEOPS 'think u know' online safety website and other useful online safety organisations. The pupils' page signposts pupils to an age appropriate 'think u know' activity to teach online safety.

3. Managing Internet Access

3.1. Information system security

School ICT systems will be monitored regularly to identify unauthorised access and potential malicious network activity.

● Virus protection will be updated regularly.
● Security strategies will be discussed with the DSL and with the Local Authority
● All staff will use the appropriate username and passwords to ensure system security. It is their responsibility to ensure that they maintain security and control of these.
● All staff are responsible for any data that they carry between school and home. This data should be password protected and not stored on a home system. Staff are responsible to model safe behaviour in their own use of technology e.g. use of passwords, logging-off, copyright, use of content.

3.2 E-mail

● **School will provide staff with an email account for their professional use e.g. name@wreningham.norfolk.sch.uk**
● Pupils and staff may only this approved e-mail accounts on the school system name@wreningham.norfolk.sch.uk
● Pupils must immediately tell a teacher if they receive offensive e-mail.
● Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
● Staff to pupil email communication must only take place via a school email address or from within the school learning platform (such as Google Classroom) and will be monitored.
● Incoming e-mail should be treated as suspicious, and attachments not opened unless the author is known.

The school will consider how e-mail from pupils to external bodies is presented and controlled.

3.3 Published content: the School Website, Facebook

The contact details on the Website, Facebook and Twitter accounts should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.

Rob Hodge (class 4 teacher/ computer subject lead) will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.4. Publishing photographs, images and work

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by their name unless with full permission of the parents. The school will look to seek to use group photographs rather than full-face photos of individual children.

● Pupils' full names will be avoided on the Website, Facebook and Twitter as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
● Written permission from parents or carers will be obtained before photographs or images of pupils are published.
● Written permission from adults will be obtained before their names, photographs or images of themselves are published.
● Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

3.5. Social networking and personal publishing on the school learning platform

● The school will control access to social networking sites and consider how to educate pupils in their safe use e.g. use of passwords.
● All users will be advised never to give out personal details of any kind which may identify them, anybody else or their location.
● Pupils, parents and staff will be advised on the safe use of social network spaces

● Staff will be advised of their roles and responsibilities under the pay and conditions of service. This includes appropriate use of social media and how it could be viewed.
● Pupils will be advised to use nicknames and avatars when using social networking sites.

Cyberbullying, the use of IT, particularly mobile phones, to deliberately hurt or upset someone, is not tolerated. All incidents will be recorded and sanctions may be applied to the perptrator.

3.6 Managing filtering
● The school will work in partnership with Norfolk Children's Services to ensure systems to protect pupils are reviewed and improved.
● If staff or pupils come across unsuitable on-line materials, the site must be reported to the nominated member of staff.
●The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.7 Managing emerging technologies
● Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

3.8. Other devices
● Only school owned cameras/devices can be used for taking photographs/videos in lessons and educational activities and visits.
● Staff will secure their personal devices and not use them during designated teaching time.
● Staff will not use phones for photographs. Personal devices must only be used in an absolute emergency
● The sending of abusive, offensive or inappropriate material is forbidden. Such events will be investigated by the designated persons under the appropriate code of conduct
● Staff should not share personal telephone numbers or contact details with pupils and parents as part of their role.

3.9. Protecting personal data
● Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and our Data Protection Policy.

4. Policy Decisions

4.1. Authorising Internet access
● All staff must read and sign the 'Staff Code of Conduct' and 'Acceptable Use Policy' before using any school ICT resource.
● Parents will be asked to sign and return a consent form.
● The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
●Pupils must agree to comply with the Responsible Internet Use statement before being granted Internet access.
● Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' form before being allowed to access the Internet on the school site.

Assessing risks
● The school will take all reasonable precautions to prevent access to inappropriate material. 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. Neither the school nor Norfolk Children's Services can accept liability for the material accessed, or any consequences of Internet access.
● The school will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate and effective.

4.3. Classification of Online Risks - the 4Cs

The four key categories of risk
Our approach to online safety is based on addressing the following categories of risk:
● Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
● Contact – being subjected to harmful online interaction with other users, such as child-to-child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
● Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
● Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

4.4. Handling Online Safety complaints
● Complaints of Internet misuse by children will be dealt with by the DSL/ Headteacher who will be assisted by the Computing Coordinator.
● Any complaint about staff misuse must be referred to the Headteacher.
● Complaints of a child protection nature must be referred to the DSL and dealt with in accordance with school's child protection procedures.
● Pupils and parents will be informed of the complaints procedure.
● Pupils and parents will be informed of consequences for pupils misusing the internet

4.5. Community use of the Internet
● All use of the school internet connection by community and other organisations shall be in accordance with the school Online Safety policy. Staff will also follow the relevant staff code of conduct sections.

5. Communication

5.1. Introducing the Online Safety policy to pupils
● Appropriate elements of the Online Safety policy will be shared with pupils
● Online Safety rules will be posted in all networked rooms, where there is pupil use of a computer.
● Pupils will be informed that network and Internet use will be monitored
● The issues around Online Safety are specifically planned for as part of the curriculum content in each year group

5.2. Staff and the Online Safety policy
All staff will be given the School Online Safety Policy and its importance explained
● All staff must read and sign the 'Acceptable Use Policy' before using any school technology.
●Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
● Staff who manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support
● Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school web site.
● Parents and carers will from time to time be provided with additional information on Online Safety.
● The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school and again in at the start of Key Stage 2.

Together Everyone Achieves More
Wreningham School is committed to Safeguarding
And promoting the Welfare of children

THE CHURCH OF ENGLAND
Diocese of Norwich

KS2 Pupils
Wreningham V.C. Primary school

Parent / carer name:……

Pupil name: ……..

Pupil's registration class: ……

As the parent or carer of the above pupil(s), I grant permission for my child to have access to use the Internet and other ICT facilities at school.

I know that my daughter or son has signed the form overleaf to confirm that they will keep to the school's rules for responsible ICT use, outlined in the ICT Code of Conduct/ Acceptable Use Policy ('Think then Click'). I also understand that my son/daughter will be informed if the rules have to be changed during the year. I know that the latest copy of the Online Safety Policy is available at ***http://www.wreningham.norfolk.sch.uk/school-policypage.html*** and that further advice about safe use of the Internet can be found at https://www.thinkuknow.co.uk/.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, employing appropriate teaching practice and teaching online safety skills to pupils.

I understand that the school can check my child's computer, and the websites they visit. I also know that the school may contact me if there are concerns about my son/daughter's online safety or online behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

Parent/carer signature:…….

Date:…….

Together Everyone Achieves More

Wreningham School is committed to Safeguarding
And promoting the Welfare of children

Reception /KS1

Wreningham V.C. Primary school

Parent / carer name :……

Pupil name: ……..

Pupil's registration class: ……

As the parent or carer of the above pupil(s), I grant permission for my child to have access to use the Internet and other ICT facilities at school.

The school has adopted the 'Think Then Click' policy with regard children's use of computing and the internet (see over leaf). A copy of the Online Safety Policy is available at ***http://www.wreningham.norfolk.sch.uk/school-policypage.html***.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but understand the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, employing appropriate teaching practice and teaching online safety skills to pupils.

I understand that the school can check my child's computer files, and the websites they visit. I also know that the school may contact me if there are concerns about my son/daughter's online safety or online behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

Parent/carer signature:……

Date:…….


Think then Click

Rules for Class 1 and 2 to help us stay safe on the Internet

We ask permission before using the Internet.

We can click on the buttons or links when we know what they do.

We can search the Internet when supervised by an adult.

We always ask if we get lost on the Internet.

We tell an adult if we see anything we are uncomfortable with or not sure about.

Rules for Class 3 and 4 to help us stay safe on the Internet

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We will only email if required as part of a required lesson.
- We send e-mails that are polite and friendly.
- We never tell anyone personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We never use Internet chat rooms or social media in school unless as part of a required lesson.

Pupil's Agreement I have read and I understand the school Online Safety Rules.

- I will use the computer, network, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Name:	Date:

Wreningham VC Primary School

ACCEPTABLE USE POLICY FOR ANY ADULT WORKING WITH LEARNERS

The policy aims to ensure that any communications technology is used without creating unnecessary risk to users whilst supporting learning (this includes a wide range of systems e.g., mobile phones, digital cameras, laptops and tablets).

I agree that I will:
● only use, move and share personal data securely.
● respect the school network security.
● implement the school's policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability, and validity of sources.
● respect the copyright and intellectual property rights of others.
● Only use the approved email system for any school business.
● only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public-facing site.
● only give permission to pupils to communicate online with trusted users.
● use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues.
● not use or share my personal (home) accounts/data (eg Facebook, email, eBay etc.) with pupils
● set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs).
● report unsuitable content and/or ICT misuse to the named e-Safety officer.
● promote any supplied E-safety guidance appropriately.
● not install any hardware or software on any school owned device without the permission of the headteacher.

- **I know that anything I share online may be monitored.**
- **I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.**
- **Mobile phones with cameras will not be used in school to take a photo of children.**

I agree that I will not:
● visit internet sites, make, post, download, upload or pass on material, remarks, proposals or comments that contain or relate to:
- inappropriate images
- promoting discrimination of any kind
- promoting violence or bullying
- promoting racial or religious hatred
- promoting illegal acts
- breach any Local Authority/School policies, e.g., gambling
● do anything which exposes others to danger.
● post any other information which may be offensive to others.
● forward chain letters breach copyright law.
● use personal digital recording equipment including cameras, phones, or other devices for taking/transferring images of pupils or staff without permission.

● store images or other files off-site without permission from the head teacher or their delegated representative.

I will ensure that any private social networking sites, blogs, etc. that I create or actively contribute to, do not compromise my professional role.

I understand that data protection policy requires me to keep any information I see regarding staff or pupils which is held within the school's management information system private, secure, and confidential. The only exceptions are when there is a safeguarding issue, or I am required by law to disclose such information to an appropriate authority.

I accept that my use of the school ICT facilities may be monitored, and the outcomes of the monitoring may be used.

SIGNED	
NAME IN BLOCK CAPITALS	
DATE	

Online Safety Checklist/ Basic Audit

This checklist can be used to carry out a very simple audit of the online safety provision in your school.
It is recommended that a more thorough audit is carried out using the 360 Degree self-review online tool. It is freely available through this web link:
http://swgfl.org.uk/products-services/esafety/services/360
This 360 audit is currently being worked through by the Computing Co-ordinator – any recommended plans of action stemming from the audit will be identified and timescales for implementation established. (02.05.2024)

The responsible member of the Senior Leadership Team is: Mr R Jones	
The responsible member of the Governing Body is: Nicola Duffie (safeguarding)	
Has the school got an online safety Policy that allies with Norfolk guidance?	**Y**
When was the policy updated/reviewed? 16th April 2024	
The school online safety policy was agreed by governors on: 17th April 2024	
How is the policy made available for staff? : Copy in Staffroom and online on website	
How is the policy made available for parents/carers?: Available in 'Policies' page on school website	
Is a clear, progressive online safety education programme in place for all pupils? Online safety progression is taught through learning objectives relating to online safety within the Purple Mash Computing Scheme of Work. Within the scheme, there are additional opportunities to reference safe online practices within lessons that are not specifically noted as a learning objective of the lesson. Additional online safety is delivered through planned RSHE online safety teaching and start of term refresh of the SMART online safety approach.	**Y**
Are all pupils aware of the School's ICT Code of Conduct (Think then Click) /Acceptable Use Policy? KS2 pupils refresh and sign annually.	**Y**
Are online safety rules displayed in all rooms where technologies are used and expressed in a form that is accessible to all pupils?	**Y**
Has up to date online safety training been provided within the last year for staff? Staff Meeting from Norfolk Education Online Safety Professional – September 2022.	**Y**
Is there a clear procedure for a response to an incident of concern?	**Y**
Do all staff receive and sign an ICT Code of Conduct on appointment?	**Y**
Do parents/carers sign and return an agreement that their child will comply with the School ICT Code of Conduct/Acceptable Use Policy? – yearly refresh in parents evening week before autumn half-term.	**Y**
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	**Y (**Visitors as required)
Is Internet access provided by an Internet service provider which complies with DfE/NEN requirements?	**Y**
Have online safety materials from CEOP been obtained?	**Y**
Is personal data collected, stored and used according to the principles of GDPR?	**Y**
Where appropriate, have teaching and/or technical members of staff attended training on the school's filtering system?	**N/A**

Wreningham V.C. Primary School

Ashwellthorpe Road
Wreningham
Norfolk
NR16 1AW
Tel / Fax: (01508) 489355
E mail: office@wreningham.norfolk.sch.uk

Headteacher: Mr R Jones M.A.

Monday 6 September, 2021

Photographs and Video Consent Form

Dear Parents,

This consent form is with regard photographs and video consent in school and is consistent with our Online Safety Policy. Photographs and videos will only be collected and stored with a documented lawful basis. They will be used where they are deemed essential for performing the public task of the school, for example for assessment purposes e.g. EYFS including learning new skills and feedback.

Where photographs are required for other purposes, these purposes will be documented and explicit consent sought. The retention period for photographs and videos is documented in the school's retention policy. At the end of the retention period photographs will either be destroyed, or may be retained for archiving purposes in the public interest.

We recognise that during the course of the school year there may be opportunities to publicise some of the activities your child is involved in e.g. class performances, Christmas plays, Sports Day, school excursions and residential trips. These activities may well involve filming or photographing the children. As a school we welcome these opportunities and hope that you do too. There may also be occasions when we arrange photography for our own purposes, such as displays and school brochures.

Before using any photographs of your child we need your permission. Please read the statements below, then sign and date the form where shown. At all times we are committed to the safeguarding of all the children in our school. Photographs that include an individual pupil will be published only if they comply with the school rules i.e. photographs will not clearly identify individuals in that only the first name will appear beside any photographs to be published: the full name will not be used.

We collect and use photographs for the following purposes (please tick the box to confirm you agree to the use of photographs for each purpose):

	Yes	**No**
For display in access-controlled areas of the school (such as corridors, classrooms).		
For display in public areas of the school (such as the school office, staffroom).		
For use in the school newsletter and other documents (such as the prospectus).		
For use on the school Website.		
School photographs can be provided to the media for publication or broadcast.		

If, at any time, you wish to withdraw consent, please ask the school office for a consent withdrawal form.

Parents' Photo Policy Statement
Where appropriate, we believe parents have the right to 'capture' memorable moments within their children's school lives in photographs and/or video. When parents attend events and performances within school, they should make every effort to only take photographs featuring their own children. Any photographs, video or recordings must be kept for your personal family use only. This means that they must not be:

- Shared on any social media website or platform.
- Shared with any third-party organization
- Broadcast or shown in public
- Used in published material

By signing and returning this form I confirm I have provided consent freely and I have read and understood the information including the Parents' Photo Policy Statement .

Parent's signature…….. Date……/……/……

Name of Child…….

THIS FORM MUST BE RETURNED TO THE SCHOOL OFFICE

THINK BEFORE YOU POST

Here are some top tips to help;

- Keep your device secure –do not share log-in information or passwords and check your settings and who can view your content
- Don't share your personal details like your name, date of birth, age, address or school and think about posting content with school logos or door number in the photo
- Think about who you are sending requests to and receiving them from – do you know them in real life? Only add people you know in real life.
- Think before you post – once the content is in a public space it can be shared with anyone
- Think about who you are talking to – people can trick you into trusting them and sharing your information
- Fake accounts – You may be asked to meet up with someone who is pretending to be someone else. Don't arrange to meet anybody you've only spoken to online.

If you need us

We have launched a new phone line and text message service for you to use. We hope you are feeling happy and safe at home, however if you're feeling unsafe or scared, then don't keep it to yourself. We're here to help you!

Text on: 07480 635060
Call on: 0344 800 8029

Norfolk Safeguarding Children Partnership (NSCP) is here to help keep children safe at home. The partnership includes Norfolk Constabulary, Norfolk County Council's Children's Services and Norfolk Children and Young People's Health Services.

You can also find more support and advice at:

norfolklscb.org I norfolk.police.uk I parentsprotect.co.uk I thinkuknow.co.uk I

Norfolk Safeguarding Children Partnership