Together **E**veryone **A**chieves **M**ore

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

THE CHURCH
OF ENGLAND
Diocese of Norwich

Wreningham V.C. Primary school

Online Safety Policy

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 Jon Gent

(This policy is based on the Norfolk Model Online Safety Policy)

Writing and reviewing the Online Safety policy

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

- ➤ Ofsted inspectors will always make a written judgement under leadership and management about whether or not the arrangements for safeguarding children and learners are effective.

- ➤ The school will identify a member of staff who has an overview of Online Safety, this would usually be the Designated Safeguarding Lead (DSL).

- ➤ Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by the senior teacher and approved by governors.

- ➤ The Online Safety Policy and its implementation will be reviewed annually

- ➤ The Online Safety Policy was discussed by Staff on: 15/3/17

- ➤ The Online Safety Policy was discussed by the School Council on 28/3/17

- ➤ The Online Safety Policy was revised by: Mr R Jones, Mr Hodge & Mrs Osborn

- ➤ It was approved by the Governors on: 27/3/17

- ➤ Date of next review: Spring Term, 2018

Contents

1. Introduction and Overview

- Rationale and Scope
- How the policy is communicated to staff/pupils/community
- Handling concerns
- Reviewing and Monitoring

2. Education and Curriculum

- Pupil online safety curriculum
- Staff and governor training
- Parent/Carer awareness and training

3. Incident Management

4. Managing the IT Infrastructure

- Internet access, security and filtering
- E-mail
- School website
- Cloud Environments
- Social networking

5. Data Security

- Management Information System access and data transfer

6. Equipment and Digital Content
- Bring Your Own Device Guidance for Staff and Pupils
- Digital images and video

Guidance and Example documents (separate documents):

Legal Framework

Example Pupil ICT Code of conduct

Example Staff, Governor, Visitor ICT Code of conduct

Example Parental/Carer Permission: Use of digital images – photography and video

Example Parent/Carer ICT Code of Conduct agreement form (Feb 2016)

Guidance for schools: Parents & Carers use of photography and filming at school events

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Wreningham School with respect to the use of technologies.

- Safeguard and protect the children and staff.

- Assist school staff working with children to work safely and responsibly with technologies and to monitor their own standards and practice.

- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of technologies for educational, personal or recreational use for the whole school community.

- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other school policies].

- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of Wreningham School community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school technologies, both in and out of Wreningham School.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- **Policy to be posted on the school website.**

- **Policy to be part of school induction pack for new staff, including information and guidance where appropriate**

- **All staff must read and sign the 'Staff Code of Conduct' before using any school technology resource**

- Regular updates and training on online safety for all staff, including any revisions to the policy

- ICT Code of Conduct (previously referred to as an Acceptable Use Policy) discussed with staff and pupils at the start of each year. ICT Code of Conduct to be issued to whole school community, on entry to the school.

Handling Concerns

- The school will take all reasonable precautions to ensure online safety is in line with current guidance from the Department for Education (DfE)

- Staff and pupils are given information about infringements in use and possible sanctions.

- Designated Safeguarding Lead (DSL) acts as first point of contact for any safeguarding incident whether involving technologies or not

- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the concern is referred to the Chair of Governors

Review and Monitoring

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy).

- The online safety policy will be reviewed annually **or** when any significant changes occur with regard to the technologies in use within the school

- There is widespread ownership of the policy and it has been agreed by the Senior Teacher and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience

- will remind students about their responsibilities through the pupil ICT Code of Conduct/ Acceptable Use Agreement

- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright

- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights

- has the front page of its website designed to sign post parents and children to the kidSMART website with information for all users about keeping safe online.

Staff and governor training

This school:

- makes regular up to date training available to staff on online safety issues and the school's online safety education program

- provides, as part of the induction process, all staff [including those on college placement and work experience] with information and guidance on the Online Safety Policy and the school's ICT Code of Conduct/ Acceptable Use Agreements

Parent/Carer awareness and training

This school:

- provides information for parents/carers for online safety on the school website

- parents/carers are issued with up to date guidance on an annual basis

3. Incident management

In this school: there is strict monitoring and application of the online safety policy, including the ICT Code of Conduct/AUP

- support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Police, Internet Watch Foundation) in dealing with online safety issues

- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school

- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible

- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

- we will immediately refer any suspected illegal material to the appropriate authorities – i.e. Police, Internet Watch Foundation and inform the LA

4. Managing IT and Communication System

Internet access, security and filtering

In this school:

- we follow guidelines issued by the Department for Education to ensure that we comply with minimum requirements for filtered broadband provision

E-mail

This school

- Provides staff with an email account for their professional use, e.g. nsix.org.uk and makes clear personal email should be through a separate account
- We use anonymous e-mail addresses, for example head@, office@

- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.

- Will ensure that email accounts are maintained and up to date

Pupils email:

- We use school provisioned pupil email accounts that can be audited

- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff email:

- Staff will use LA or school provisioned e-mail systems for professional purposes

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

- Never use email to transfer staff or pupil personal data unless it is protected with secure encryption. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website

- The school web site complies with statutory DfE requirements

- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;

- Photographs of pupils published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.

- Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open up their own spaces to their pupils, but to use the schools' preferred system for such communications.

- The use of any school approved social networking will adhere to ICT Code of Conduct/AUP

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.

- Children are required to sign and follow our [age appropriate] pupil ICT Code of Conduct/AUP

How will Cyberbullying be managed?

Cyberbullying is defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007.

- Children are required to sign and follow our [age appropriate] pupil ICT Code of Conduct/AUP

- It is essential that pupils, Wreningham staff and parents/carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse.

- Promoting a culture of confident users will support innovation and safety. DCSF and Childnet have produced resources and guidance that will be used to give practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying

- Cyberbullying (along with all forms of bullying) will not be tolerated in school. All incidents of cyberbullying reported to the school will be recorded.

- There are clear procedures in place to investigate incidents or allegations of bullying:

• Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

• The school will take steps to identify bullying behaviour, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Sanctions for those involved in Cyberbullying may include: The perpetrator will be asked to remove any material deemed to be inappropriate or offensive. A service provider may be contacted to remove content. Internet access may be suspended at school for the user for a period of time. Parent/carers will be informed and the Police will be contacted if a criminal offence is suspected.

Parents/Carers:

- Parents/carers are reminded about social networking risks and protocols through our parental ICT Code of Conduct/AUP and additional communications materials when required.

5. Data Security

Management Information System access and data transfer

- Please use guidance from the [Information Commissioner's Office](#) to ensure that you comply with your responsibilities to information rights in school

6. Equipment and Digital Content

Bring Your Own Device Guidance for Staff and Pupils

- Please use guidance from [The Education Network (NEN) around Bring Your Own Device](#)
- Mobile phones and associated cameras will not be used during lessons or formal school time where pupils are present except as part of an educational activity.
- Following Early Years guidance mobile phones with cameras are not permitted in the Foundation stage during lessons or formal school time.
- The sending of abusive, offensive or inappropriate material is forbidden.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care will be taken with their use within the school use.
- Staff should not share personal telephone numbers with pupils and parents. (A school phone will be provided for staff where contact with pupils is required).

Digital images and video

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school (or annually)

- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs

- Staff sign the school's ICT Code of Conduct/AUP and this includes a clause on the use of personal mobile phones/personal equipment

- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use

T̲ogether E̲veryone A̲chieves M̲ore
**Wreningham School is committed to Safeguarding
And promoting the Welfare of children**
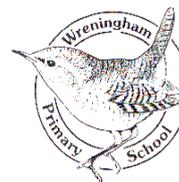
Wreningham V.C. Primary school

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, school email 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 may 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, safe access to email, 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 do not use Internet chat rooms.

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:

Staff, Governor and Visitor - ICT Code of Conduct/Acceptable Use Policy
Wreningham VC Primary School

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This code of conduct is provided to ensure that all users are aware of their responsibilities when using any form of ICT provided by or directed by Norfolk County Council. All such users will be issued with this code of conduct. Any concerns or clarification should be discussed with the headteacher.

➢ All staff, Governors and visitors understand that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, laptops and tablets

➢ All staff understand that it is a disciplinary offence to use the school ICT system and equipment for any purpose not permitted by its owner.
   (Teaching Staff http://www.schoolspeoplenet.norfolk.gov.uk/Teaching-Staff/Working-in-a-Norfolk-School/Resolving-Issues/Disciplinary/index.htm
   Support Staff http://www.schoolspeoplenet.norfolk.gov.uk/Support-Staff/Working-in-a-Norfolk-school/Resolving-Issues/Disciplinary/index.htm)

➢ All staff, Governors and visitors will not disclose any passwords provided to them by the school or other related authorities.

➢ All staff, Governors and visitors understand that they are responsible for all activity carried out under their username

   ➢ Staff, Governors and visitors will not install any hardware or software on any school owned device without the permission of the headteacher.

➢ All staff, Governors and visitors understand that their permitted use of the Internet and other related technologies is monitored and logged and will be made available, on request, to their Line Manager or Head teacher in line with any disciplinary procedures. This relates to all school owned devices, including laptops provided by the school.

➢ All staff, Governors and visitors will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for uses permitted by the Head or Governing Body.

➢ All staff, Governors and visitors will ensure that all their school generated electronic communications are appropriate and compatible with their role.

- All staff, Governors and visitors will ensure that all data is kept secure and is used appropriately as authorised by the Head teacher or Governing Body. If in doubt they will seek clarification. This includes taking data off site.

- Personal devices must only be used in the context of school business with explicit permission of the Headteacher.

- All staff, Governors and visitors using school equipment will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- All staff, Governors and visitors will only use the approved email system(s) for any school business

- Images will only be taken, stored and used for purposes in line with school policy. Images will not be distributed outside the school network without the consent of the subject or of the parent/carer, and the permission of the Head teacher.

- All staff, Governors and visitors will comply with copyright and intellectual property rights.

- All staff, Governors and visitors will report any incidents of concern regarding staff use of technology and/or children's safety to the Senior Designated Professional or Head teacher in line with the school's Safeguarding Policy.

I acknowledge that I have received a copy of the ICT Code of Conduct.

Full name:…………………………………………………………….…(printed)

Job title:………………………………………………………………………….…

Signature:……………………………………………**Date:**……………………

Online Safety Checklist/ Basic Audit - Spring Term 2017

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

The responsible member of the Senior Leadership Team is: **Rob Hodge**	
The responsible member of the Governing Body is: **Miriam Osborn**	
Has the school got an online safety Policy that allies with Norfolk guidance?	**Y**
When was the policy updated/reviewed? **Spring Term 2017**	
The school online safety policy was agreed by governors on: **27/3/17**	
How is the policy made available for staff? : **Y**	
How is the policy made available for parents/carers?: **Y**	
Is a clear, progressive online safety education programme in place for all pupils?	**In progress**
Are all pupils aware of the School's ICT Code of Conduct/Acceptable Use Policy?	**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?	**N but date arranged**
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?	**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 the Data Protection Act, following guidance provided by the ICO?	**Y**
Where appropriate, have teaching and/or technical members of staff attended training on the school's filtering system?	**N/a**
Are staff with responsibility for managing network access and monitoring adequately supervised by a member of SLT?	**Y**

Wreningham V.C. Primary School

Ashwellthorpe Road
Wreningham
Norfolk
NR16 1AW
Tel / Fax: (01508) 489355
E mail: office@wreningham.norfolk.sch.uk
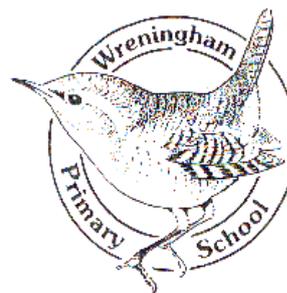
Head Teacher: Mr R Jones M.A.

_____

Friday 16 March 2017

Dear Parents,

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. Thank you.

1. Parent's Consent for Web Publication of Work and Photographs
I agree that, if selected, my child's work may be published on the school Website. I understand that photographs that include my child will be published **only** if they comply with the school rules that photographs will not clearly identify individuals in that their full name will not be used. We also may display photographs of the children inside the school building.

Can we use your child's photograph and work in this way? Please circle Yes or No

2. We occasionally send photographs to the news media, especially the local press, to celebrate a school event. It is understood that only my child's first name will appear beside any photographs to be published.

Can we use your child's photograph in this way?   Please circle Yes or No

3. We believe parents have the right to record memorable moments within their children's school lives in photographs and/or video, where appropriate. When parents attend events and performances within school, they may take photographs of their children for their own use. **We ask parents not to post the footage on social media sites.**

Can your child's photograph be taken in this way?   Please circle Yes or No

Parent's signature…………………………………..   Date…………/………/………

Name of Child………………………………………………….

2016/17 Cycle A Ongoing Online safety embedded - Re-visited explicitly in session at beginning of each term and on Internet Safety Day (Feb)

	Autumn 1 (7) Out of this world	Autumn 2 (7) Festivals	Spring 1 (6) Take one picture	Spring 2 (5) Kings and Queens	Summer 1 (6) Amazing animals and Plants	Summer 2 (7) Great lives
Class 1						
Class 2	We are celebrating-Create Christmas card	We are photographers – Taking , selecting/editing	We are TV chefs – Instructions-filming steps of recipe	We are collectors – Finding images on web - plants	We are Astronauts Simple Coding onscreen	We are celebrating-Create Christmas card
Class 3	Introduction to Programming – Scratch concepts	Computational Thinking Designing an educational game – Planning and practice	Bug Hunters Hunting down bugs and fixing programs Scratch	We are opinion pollsters Collecting and analyzing data Goggle Forms	Video Performance We are presenters-Using Moviemaker	We are communicating safely on the internet –
Class 4	Programming Intro Computing coding skills	Programming Extend Interactive adventure	Creativity – Movie Maker A journey through dreamscape	Networks – Webpage Create an safety webpage	Computer art Fusing geometry and art Coding art with scratch	Cresting a virtual space Sketchup design – We are architects

2017/18 Cycle B Ongoing Online safety embedded - Re-visited explicitly in session at beginning of each term and on Internet Safety Day (Feb)

	Autumn 1 (7) **Incredible Islands**	Autumn 2 (7) **Festivals**	Spring 1 (6) **Momentous Moments from the past**	Spring 2 (5) **Magnificent Materials**	Summer 1 (7) **Spirit of Norfolk**	Summer 2 (6 ½) **Under the Sea**
Class 1						
Class 2	We are zoologists- Recording bug hunt data	We are Painters– Illustrate a xmas story	We are treasure hunters - controlling programmable toys	We are storytellers- Create a talking book	We are researchers – Finding out about our historical people	We are zoologists- Recording bug hunt data
Class 3	Year 3 - Introduction to Programming – Scratch concepts Year 4 – interactive Toy design	Computational Thinking Designing an educational game – Planning and practice Year 4 - Extended	We are musicians – Producing Digital music- Audacity software	We are meteorologists Presenting the weather Excel – Powerpoint On IWB presentation	Create a Teaching tool – Scratch – design an interactive environment game.	Wikis and Blogs – Creating our own – Hobbies and interests.
Class 4	Advanced Programming Ideas Reusability Creating AI	Computational thinking Cracking Codes	Control Systems	Planning an app- Design and planning Prototyping	App developing – Simple mobile phone app	Market your app – advertising