E-SAFETY POLICY

Date for adoption: November 2017

E-Safety Policy –

Introduction

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's e-safety policy should operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

This policy has been strongly influenced by the work of the Kent e-Safety team.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible Computing use by all staff and students; 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 including the effective management of filtering systems

1.0 School e-safety policy

1.1 Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for Computing and for child protection.

- The school's e-Safety Coordinator is also the Head Teacher. He works in close co-operation with all Subject Leaders.
- Our e-Safety Policy has been written by the E-Safety Governor and Head Teacher who is the designated Safeguarding Lead. It has been agreed by the staff and governors.
- The e-Safety Policy will be reviewed Annually – or sooner if needs arise .

1.2 Teaching and learning

1.2.1 Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

1.2.3 Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- All pupils will have the ability to Block and Lock their computer screen to hide any content they are concerned about until a teacher has checked it.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

1.2.4 Pupils will be taught how to evaluate Internet content

If pupils discover unsuitable sites, this should be reported immediately to the class teacher who will record the URL (address), time, date and content which will then be reported to the school Computing Subject Leader.

- Staff should ensure that 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.

1.3 Managing Internet Access

1.3.1 Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses Broadband for Internet delivery, but access is filtered and protected in line with the needs of a Primary School.

1.3.2 E-mail

- Pupils may only use approved e-mail accounts on the school system. Children are not allowed access to personal e-mail accounts or chat rooms whilst in school.
- 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.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

1.3.3 Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Where the School Newsletter features children's names, the names will be replaced with initials before the Newsletter is hosted on the school website.

1.3.4 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. Children's names are never associated with any images used.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

1.3.5 Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Pupils are taught never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils. We actively discourage the use of Facebook, as it has a user policy of 13+.

1.3.6 Managing filtering

- The school will work in partnership with the service provider to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E-Safety coordinator and Computing Subject Leader. All such events will be logged, along with any action taken. The log (edited to remove individual's names) will be regularly reviewed by the E-Safety Committee.
- Senior staff will ensure that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

1.3.7 Managing videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- External IP addresses should not be made available to other sites.

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing should be supervised appropriately for the pupils' a and would normally be a group or class activity.

1.3.8 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.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Where permission is given for pupils to use Personal Technology it will only be for research or curriculum specific tools, eg a Dictionary or Thesaurus. The sending of Texts, Emails or IM is strictly forbidden.

1.3.9 Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

1.4 Policy Decisions

1.4.1 Authorising Internet access

- The school will maintain a current record of all pupils who are granted Internet access. This is updated annually in September, and for each pupil joining mid year
- All staff, including Teaching Assistants and Supply Teachers must read and sign the Responsible Internet Use Policy (RIUP) before using any school Computing resource or E-Mail account.
- At FS/Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents and pupils will be asked to sign and return a consent form agreeing to comply with the school's Responsible Internet Use Policy.

1.4.2 Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of 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, and parents much accept this when signing the Responsible Internet Use agreement.
- The headteacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

1.4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Sanctions within the school behaviour policy include:
    - interview/counselling by class teacher / headteacher;
    - informing parents or carers;
    - removal of Internet or computer access for a period.
- Depending on the nature of the compliant the school may choose to involve the police 'Safer Communities' team who will work with the children and families involved.

1.4.4 Community use of the Internet

- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- Parents using school computer equipment must sign an RIUP consent form prior to use

1.4 Communications Policy

1.5.1 Introducing the e-safety policy to pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Advice on e-Safety will be introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet use.

1.5.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff have access to a school phone where contact with pupils is required.
- Our staff Code Of Conduct adheres to the latest national and local 'Safeguarding Children' guidance.

1.5.3 Enlisting parents' / carers' support

- Parents' / carers' attention will be drawn to the School e-Safety Policy in newsletters.
- The school will hold parent workshops to raise awareness of E-Safety and computing in school – especially as technology continues to advance.

Appendix 1: Internet use - Possible teaching and learning activities

Activities	**Key e-safety issues**	**Relevant websites**
Creating web directories to provide easy access to suitable websites.	Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	
Using search engines to access information from a range of websites.	Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Ask Jeeves for kids Yahooligans CBBC Search Kidsclick Picsearch safesearch **NOT Google images**
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.	E-mail a children's author E-mail Museums and Galleries E-Mail a pre-arranged link school or class.
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	School website
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	School website
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	GridClub Cybercafe (Thinkuknow)

Appendix 2 - E-Safety Audit

This quick audit will help the Senior Leadership Team (SLT) assess whether the basics of e-Safety are in place **to support a range of activities that might include those detailed within Appendix 1.**

The school has an e-Safety Policy	**Y**
Date of latest update:	November 2017
The Policy was agreed by governors on:	**[To Add]**
The Policy is available for staff	Y
And for parents	Y
The Designated Senior Lead for Child Protection is	Mr Thorpe
The e-Safety Coordinator is	Mr Thorpe
How is e-Safety training provided?	Via Safer Internet Day and Newsletter
Is the Think U Know training being considered?	**Y**
All staff sign a Responsible Internet Use Agreement.	**Y**
Parents sign and return an agreement that their child will comply with the school Responsible Internet Use statement.	**Y**
Rules for Responsible Use have been set for students:	Y
These Rules are displayed in all rooms with computers.	Y
Internet access is provided by an approved educational Internet service provider and complies with DfE requirements for safe and secure access.	**Y**
The school filtering policy has been approved by SLT.	**Y**
An Computer security audit has been initiated by SLT, possibly using external expertise.	Y – internal only
School personal data is collected, stored and used according to the principles of the Data Protection Act.	**Y**
Staff with responsibility for managing filtering and network access monitoring work within a set of procedures and are supervised by a member of SLT or E-Safety Committee.	N/A. Handled by SWGfL
Have these staff attended training on the filtering and monitoring systems?	N/A

Responsible Internet Use

These rules help us to be fair to others and keep everyone safe.

- I will ask permission before using the Internet.
- I will use only my login and password.
- I will only open or delete my own work.
- If I take any photos during a school activity, I will not upload them to an Internet site.
- I understand that I must not bring into school and use software or files without permission.
- I will only e-mail and open attachments from people my teacher has approved.
- The messages I send will be polite and sensible.
- I understand that I must never give my home address or phone number, or arrange to meet someone.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I understand that the school may check my computer files, e-mails I send and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. The South West Grid for Learning (SWGfL) monitors all Internet use and will notify the police and Local Authority if an illegal website is accessed.

Alderbury & West Grimstead
Church of England (Aided) Primary School
Head Teacher: Mr W Thorpe
Firs Road, Alderbury, Salisbury, SP5 3BD
Tel: (01722) 710464
Email: admin@alderbury.wilts.sch.uk

September 2017

Dear Parents

Responsible Internet Use

As part of your child's curriculum and the development of ICT skills, Alderbury and West Grimstead Primary School provides supervised access to the Internet. Please would you read the attached revised Rules for Responsible Internet Use and sign and return the consent form so that your child may use the Internet at school.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school Internet provider, the South West Grid for Learning (SWGfL) operates a filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.

Should you wish to discuss any aspect of Internet use in school, please telephone me to arrange an appointment.

Yours faithfully

Mr W Thorpe

Alderbury & West Grimstead

Church of England (Aided) Primary School
Responsible Internet Use

Please complete, sign and return to the school office

Pupil:	***Class:***

Pupil's Agreement

I have read and I understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and follow these rules at all times.

Signed:	***Date:***

Parent's Consent for Internet Access

I have read and understood the school rules for responsible Internet use and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	***Date:***
Please print name:	

Parent's Consent for Web Publication of Work and Photographs

I agree that, if selected, my son/daughter's work may be published on the school website. I also agree that images, sound files and video that include my son/daughter may be published subject to the school rules that this content will not clearly identify individuals and that full names will not be used.

Signed:	***Date:***

Alderbury & West Grimstead
Church of England (Aided) Primary School
Head Teacher: Mr W Thorpe
Firs Road, Alderbury, Salisbury, SP5 3BD
Tel: (01722) 710464
Email: admin@alderbury.wilts.sch.uk

E-Safety Incident Report

This event report form is compiled by:

Name:……

Title:……

Date:……

Details of incident:

Description:

Date of incident:

Time of incident:

Machine identifier:

Logon identifier:

Offending URL:

Name of person reporting incident

If not reported, how was the incident identified?

Where did the incident occur? (In school/out of school setting)

Who was involved in the incident?

Child/young person.……

Staff member.……

Other (please specify).……

Incident witnessed by: ……

Nature of incident:

Deliberate or accidental? ……………………………………………………………………………………………………

Did the incident involve material being created/viewed/printed/shown to others/transmitted to others/distributed?

Action taken:

Staff informed:

Head Teacher – Name: ……………………………………………………….Date: ……………………………………………………

E-Safety Co-ordinator – Name: …………………………………………..Date: …………………………………………………..

Child Protection Officer – Name: ……………………………………….Date: …………………………………………………..

Other – Name:……………………………………………………………………Date: …………………………………………………

Other – Name: ……………………………………………………………………..Date: ………………………………………………

Incident reported to head teacher/senior manager? (Details of any action taken)

Advice sought from Safeguarding/Social Care? (Details of any action taken)

Incident reported to Police? (Details of any action taken)

Incident reported to internal IT? (Details of any action taken)

Advice taken from RM SafetyNet (Phone **RM** Support Services: **08454 040 000**, or,
email **incident@rm.com** with full details of the vulnerability or incident. (Details of any action taken)

Disciplinary action to be taken?

E-Safety policy to be reviewed?

Incident reported to E-Safety committee? (Details of any action taken)

Evidence collected (and where retained)?

Search history?

URL?

RM call log number?

Letter to parents?

Review required? (Date)