Online Safety Policy (updated January 2019)
(*to be reviewed annually*)

Online safety encompasses Internet technologies and electronic communications such as mobile phones, tablets, laptops and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The Federation's Online Safety Policy will operate in conjunction with other policies including those for Pupil Behaviour, Anti-Bullying, Child Protection, Curriculum, Data Protection and Security and Norfolk County 'G319 Internet and email usage in schools – model guidance for schools.

Good Habits

Online 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 Online 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 using Netsweeper.

Dangers to consider

Some of the dangers they 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
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' / 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. The Federation must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The Online Safety Policy that follows explains how we intend to do this.

Why is Internet Use Important?

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 Federation's management information and administration systems.

Internet use is part of the statutory 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 Federation has a duty to provide pupils with quality Internet access.

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.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:
• Access to world-wide educational resources including museums and art galleries;
• Inclusion in the National Education Network which connects all UK schools;
• 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

How can Internet Use Enhance Learning?

• The Federation Internet access will be designed expressly for pupil use and includes 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
• Internet access will be planned to enrich and extend learning activities
• Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity
• Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Authorised Internet Access

• All staff must read and sign the 'Acceptable ICT Use Agreement' before using any Federation ICT resource.
• Parents will be informed that pupils will be provided with supervised Internet access.
• Parents will be asked to sign and return the 'Acceptable ICT Use Agreement' which will also be signed by pupils each year

World Wide Web

• If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to Miss Frier who will investigate and take appropriate action
• The Federation will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
• Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email and online collaboration

• Pupils may only use approved e-mail accounts on the school system
• Pupils must immediately tell a teacher if they receive offensive messages
• Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
• Pupils must not access others pupil's accounts
• Whole class or group e-mail addresses should be used in school
• Access in school to external personal e-mail accounts may be blocked
• The forwarding of chain letters is not permitted

Social Networking

• Pupils will be told never to give out personal details of any kind which may identify them or their location
• Pupils should not place personal photos on any social network space
• Pupils should be told about security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
• Pupils and parents should be made aware that some social networks are not appropriate for children of primary school age

Filtering

The school will work in partnership with Internet Service Provider to ensure filtering systems are as effective as possible.

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 for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
• Staff will be issued with a school phone where contact with pupils is required.

Published Content and the Federation 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 or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate

Publishing Pupils' Images and Work

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

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the GDPR policies and procedures the Federation have in place.

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. The school cannot accept liability for the material accessed, or any consequences of Internet access.
• The school should audit ICT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate

Handling Online 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

Communication of Policy

Pupils
• Rules for Internet access will be posted in all rooms use for Internet access
• Pupils will be informed that Internet use will be monitored

Staff
• All staff will be given the School Online 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.

Parents
• Parents' attention will be drawn to the School Online Safety Policy in newsletters and on the school Web site

Communication Technologies	Staff & other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓							✓
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social times (lunchtime and after school hours)	✓							✓
Taking photos on mobile phones or personal camera devices				✓				✓
Use of hand held devices such as tablets/iPads	✓						✓	
Use of personal email address in school	✓							✓
Use of school email for personal emails		✓						✓
Use of chat rooms			✓ For professional purposes (WebEx)			✓		
Use of instant messaging			✓ For professional purposes (WebEx)			✓		
Use of social networking sites in lessons				✓				✓
Use of social networking sites in social times	✓							✓

Example of the letter sent to parents.

Acceptable ICT Use Agreement: pupils and parents

Rules for Responsible Computer and Internet Use at School

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 The Pilgrim Federation of Church of England Schools 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.

• **The school strongly recommends that children do not use social network sites such as Facebook at home, as these sites carry an age-restriction and pose a risk to children. Social networks, such as Facebook have no place in our school and so school staff should not be approached by children online.**

Please read and sign the 'Rules for Responsible Computer and Internet Use whilst at school' with your child to show your support of the school in this important aspect of our work.
• I will only access the system with my own login
• I will not access other people's files
• I will ask permission from a member of staff before using the Internet and I will only access sites approved by a trusted adult
• I will only email or message people I know or a trusted adult has approved
• The messages I send will be polite and responsible
• I will not give my home address or telephone number in any message
• I will report any unpleasant material, anything that upsets me or anything that seems 'wrong'.
• I will tell a trusted adult if I am contacted by a stranger or receive unpleasant messages.
• I understand that this would help protect other pupils and myself and that the school would need to take appropriate action.
• I understand that the school may check my computer files and may monitor my use of the internet

Sanctions
• Deliberate minor incidents in school will lead to a warning
• Serious incidents (or repeated minor incidents) will mean access to the ICT equipment or the internet is removed
• Illegal behaviour by anyone will be dealt with by the police

Parent/Guardian Name _____

Signed _____

Pupil Name _____

Signed (child) _____

Date _____

Online Safety Rules

These Online Safety Rules help to protect pupils and the Federation by describing acceptable and unacceptable computer use.

A separate set has been designed for the R/KS1 and KS2 aged children.

These are detailed below as examples and are displayed in computer areas, used as a means of reinforcing rules about the use of ICT and the internet as well as used as an aide memoire in the teaching of Online Safety to our pupils.

In addition to this, linked with Childnet International, there is a "SMART" on the internet poster that is applicable to all ages of pupils.

Online Safety Package for parents and pupils

As part of the schools responsibility to teach children online safety we use materials from the Childnet International site including online safety videos. We also use the NSPCC and Think You Know sites.

The link for some of these materials is detailed below.

http://www.childnet.com/resources/the-adventures-of-kara-winston-and-the-smart-crew/watch-full-movie

Parents are contacted to find out when is best suited to hold our Online Safety sessions and these are then organised to look at and support parents with use of internet, supervision of children on computers and the internet, benefits of using the internet and places to find help/support further related to keeping children safe online.

This policy should be looked at in accordance with the Federation Safeguarding policy.

Online Safety Rules

These rules help us to stay safe on the Internet

|	
	I will only use the Internet when an adult is with me.
	I can click on the buttons or links when I know what they do.
	I will always ask if I get lost on the Internet.
	I will tell a teacher or adult if I see anything I am unhappy with.
	I will only use my login and keep my password a secret.
	Any work I produce or display is work I would want my friends and family to see.
	I will use ICT responsibly and know these rules are to keep me safe.

Stay Safe On The Net
PUPIL RULES

When accessing the Internet and using e-mail, you must always follow the rules below:

- Log on using only your allocated username and password
- Never give your password, even to a friend
- Use the Internet only with staff permission
- Download from the Internet only with staff permission
- Never search for inappropriate information
- Never use Instant Messaging services in school such as MSN
- Never buy anything from the Internet in school
- Never send messages which could upset anyone. This is called Cyberbullying.
- Never use bad language
- Never give personal information
- Never send photographs which could identify individuals
- Never arrange a meeting with anyone on the Internet
- Report to the teacher anything which makes you feel uncomfortable
- Report any breaches of the Internet rules
- Always log off when work is completed

REMEMBER: ALL INTERNET ACCESS, including e-mail, IS MONITORED

- School rules about acceptable behaviour apply when using the Internet.
- Your teacher or headteacher will contact your parents if you break these rules.
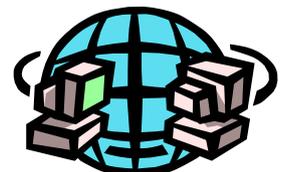
Be smart on the internet

S — **SAFE** — Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

m — **MEETING** — Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

a — **ACCEPTING** — Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

r — **RELIABLE** — Information you find on the internet may not be true, or someone online may be lying about who they are.

t — **TELL** — Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

THINK U KNOW .co.uk

www.kidsmart.org.uk

KidSMART — Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

<u>Acceptable Use Agreement: staff</u>

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 Online Safety Policy for further information and clarification.

Monitoring
The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information 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.

Incidents which appear to involve deliberate access to web sites, newsgroups and online groups that contain the following material will be reported to the police:
• images of children, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative,
• Material that breaches the Obscene Publications Act in the UK
• Criminally racist material.

The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
• I will ensure that my information systems use will always be compatible with my professional role.
• I understand that school information systems may not be used for private purposes, without specific permission from the Headteacher.
• I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
• I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager or member of senior leadership.
• I will not install any software or hardware without permission.
• I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
• I will respect copyright and intellectual property rights.
• I will report any incidents of concern regarding children's safety to the Designated Safeguarding Lead.
• I will ensure that any electronic communications with pupils are compatible with my professional role.
• I will promote online safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
• I understand that comments made in networking sites such as Facebook or Twitter should make no direct or indirect reference to our Federation, should not include images of school or children involved in school activities.
• I understand that having a social media account of any kind is my right however the content and manner in which I behave using these accounts must be in line with the professional context in which I work. No comment, picture or input should be deemed as unprofessional or bring the Federation into disrepute.

I have read, understood and agree with the Acceptable Use agreement.

Signed: ……………………………………………… Date: ………………………