GODSTONE VILLAGE SCHOOL

ONLINE SAFETY POLICY

REVEIWED: SEPTEMBER 2016

BY: RICHARD LEONARD/ HAYLEY LANCASHIRE

NEXT REVIEW: SEPTEMBER 2017

Headteacher Signature:…… Date:…….

Chair of Governors Signature:…… Date:.....

Godstone village school online safety policy

Online safety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for behaviour, safeguarding, Staff Behaviour, anti-bullying, data handling and the use of images.

Using this policy

- The school will form an online safety committee and will appoint an online safety lead.
- Our online safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The online safety policy was revised by: Hayley Lancashire/ Richard Leonard
- It was approved by the Governors on: 24th November 2016
- The online safety policy and its implementation will be reviewed annually. The next review is due: Autumn 2017
- The online safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and hand held games consoles used on the school site.
- The online safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.

Rational for online safety

- The use of computers, technology and the internet is embedded in the teaching and learning style of our school.
- We believe in educating our school community about the internet not blocking access to it. Students are given the chance to make choices as part of their learning, wherever possible.
- We recognise that there are fundamental differences between personal and professional use of technology. Our online safety policy gives guidance so as to minimise the chances of inappropriate use of the school computer systems, given that the inappropriate use of technology can have wide reaching consequences
- The online safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the school site. This includes but is not limited to workstations, laptops, mobile phones and tablets.
- The online safety Policy relates to other policies including those for Computing, Learning and Teaching, Staff Behaviour, Data Protection, Bullying, Behaviour and Child Protection.
- The online safety policy is reviewed annually by the online safety group.

Management of online safety

- The Headteacher and Online safety lead is responsible for the schools' approach to online safety.
- The school will have online safety committee which will meet once a term.
- Pupils discuss online safety as a regular agenda item at school council meetings.
- Online safety is a regular agenda item at the governors' teaching and learning committee meeting.

Communications

- All school business must be carried out using a school email address.
- Parents are allowed to email teachers on their school email accounts.
- Teachers should endeavour to reply to Parent emails within 3 days of receiving an email.
- Teachers should only reply to emails using their school email address.
- School or class Messages are to be sent to parents via Tucasi.
- Staff should use a school telephone when contacting parents or should take steps to protect their phone number (dial 141 in front of the number) if they use a personal device (see Staff Code of Conduct).

Use of images

- All photos taken in school or school activities by a member of staff or governor are to be taken on school devices.
- Photos taken in school are to be saved on to the media folder on the schools network and be deleted off the device which they were taken from.
- Parents are allowed to film and take pictures of children during class assemblies and performances, before allowing this to happen parents must informed that the images/ videos are for their personal use only and are not to be shared on social media.

- The school will take photos at school events and make them available to the school community via the school website and within newsletters. All images will be checked before publishing to ensure that all parents have agreed for their child's photograph to be shared in this way.

Managing access and security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school networks will be controlled by usernames and passwords.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform online safety policy.
- The security of school IT systems will be reviewed regularly.
- All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.
- Forwarding chain letters is not permitted.

Internet Use

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. The school will provide an age-appropriate online safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law

- Pupils will be advised not to give out personal details or information which may identify them or their location.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be shown how to publish and present information appropriately to a wider audience.
- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

E-mail

- Pupils and staff may only use approved e-mail accounts on the school IT systems.
- Staff to pupil email communication must only take place via a school email address or from within the learning platform.
- 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.
- Staff may access work emails on their own personal devices but must not save any passwords on to their devices.
- Access to email on mobile devices is only permitted via a web browser

Published content eg school web site, school social media accounts

- The contact details will be the school address, email 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

- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school web site or any school run social media as set out in Surrey Safeguarding Children Board Guidance on using images of children. http://www.surreycc.gov.uk/?a=168635
- Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Use of social media including the school learning platform

- The school has a guidelines on social media usage in the Staff Behaviour policy
- The school will control access to social networking sites, and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.
- Staff and pupils should use ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community.
- Staff should follow the guidance in the Staff Code of Conduct in relation to having parents as friends on social media.
- The school will enable pupils/students to explore and learn about online communication through the use of a safe school cloud environment.
- Staff should be aware of the expectations within part two of the Teacher standards when using social media.

Use of personal devices

- Personal equipment may not be used by staff and/or pupils to access the school IT.
- Staff must not store images of pupils or pupil personal data on personal devices.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.
- Staff may open School emails on a personal device but must ensure passwords are not saved on the personal device.

Protecting personal data

- The school has a separate Data Handling Policy. It covers the use of biometrics in school, access to pupil and staff personal data on and off site, remote access to school systems.

Policy Decisions

Authorising access

- All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, ICT technicians and governors) must read and sign the 'Staff AUP' before accessing the school IT systems (see appendix 1)
- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- In EYFS and Key Stage 1, access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials.
- In Key Stage 2, access to the internet will be with teacher permission with increasing levels of autonomy.
- People not employed by the school must read and sign a visitor AUP before being given access to the internet via school equipment (See appendix 2)
- Parents will be asked to sign and return a consent form to allow use of technology by their pupil (see appendix 3)

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 SCC can accept liability for the material accessed, or any consequences of internet access.

Handling online safety complaints

- Complaints of internet misuse will be dealt according to the school behaviour policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the schools' behavior policy.

Community use of the internet

- Members of the community and other organisations using the school internet connection will have signed a visitor AUP so it is expected that their use will be in accordance with the school online safety policy.

Communication of the Policy

To pupils

- Pupils need to agree to comply with the pupil AUP in order to gain access to the school IT systems and to the internet (see appendix 4)
- Pupils will be reminded about the contents of the AUP as part of their online safety education

To staff

- All staff will be shown where to access the online safety policy and its importance explained.
- All staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet
- All staff will receive online safety training on an annual basis

To parents

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- 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 will be offered online safety training annually

Appendix 1

Godstone Village School
Acceptable Use Policy / ICT Code of Conduct for staff members

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 policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere to its contents at all times. Any concerns or clarification should be discussed with Candida Jarrott-Chase, Headteacher.

- I appreciate that ICT includes a wide range of systems, including mobile phones, tablets, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.

- I will only use the school's email / internet / intranet / Learning Platform and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Head or Governing Body.

- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

- I understand that I am responsible for all activity carried out under my username.

- I will only use the approved, secure email system(s) for any school business.

- I will ensure that all electronic communications with parents, pupils and staff, including email, IM and social networking, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body.

- I will only take images of pupils and/or staff for professional purposes in line with school policy. I will not distribute images outside the school network/learning platform without the permission of the Head teacher.

- I will not install any hardware or software without the permission of Candida Jarrott-Chase.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- I will respect copyright and intellectual property rights.

- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

- I will support the school's Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies. I will promote online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

- I will report any incidents of concern regarding children's safety the Designated safeguarding lead Candida Jarrott- Chase, or in her absence the Deputy Designated safeguarding lead Hayley Lancashire.

- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serous infringements may be referred to the police.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Full Name…… (Printed)

Job title……

Signature…… Date……

Appendix 2

Godstone Village School

Acceptable Use Policy / ICT Code of Conduct for visitors

- I understand that I have been given use of the school internet and/or school ICT systems in order to carry out a specific job for the school
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will only use the school's email / internet / intranet / Learning Platform and any related technologies for the purpose for which I have been given access.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will not install any hardware or software without the permission of Candida Jarrott-Chase.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory whilst using the school ICT systems
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to the Head teacher or my employer.
- I will respect copyright and intellectual property rights.
- I understand that if I disregard any of the above then it will be reported to my employer and serious infringements may be referred to the police.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Full Name…… (Printed)

Company……

Signature…… Date……

Appendix 3

Godstone Village School

Parent/Carer consent form and Online Safety Rules

All pupils use computer facilities, including internet access, as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign agreements to show that the Online Safety Rules have been understood and agreed.

Parent / Carer name: ……

Pupil name: ……..…….

As the parent or legal guardian of the above pupil, I have read and understood the attached school online safety rules and grant permission for my daughter or son to have access to use the internet, school email system, learning platform and other ICT facilities at school.

I know that my daughter or son has signed an online safety agreement form and that they have a copy of the school online safety rules. We have discussed this document and my daughter or son agrees to follow the online safety rules and to support the safe and responsible use of ICT at Godstone Village School.

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 an educationally filtered service, restricted access 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 internet sites that they visit, and that if they have concerns about their online safety or e-behaviour they will contact me.

I understand the school is not liable for any damages arising from my child's use of the internet facilities.

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/Guardian signature:

……Date.....

Please complete, sign and return, via your child, to their class teacher

Appendix 4

Godstone Village School

Acceptable use of the school computers EYFS and KS1

These rules help me to stay safe on the internet

I will take care of the school computers and laptops.

I will always tell an adult before I use the computers and laptops.

I will only use the internet when I have been told I can by an adult.

I will tell a trusted adult if I see something on the internet that upsets me.

I will not tell other people important things about me.

I will always be polite and friendly when I write messages on the internet.

Acceptable use of the school computers KS2

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

- I will only use the school's computers and laptops for schoolwork and homework during lessons
- If attending Swans club , I will ask for permission to use games or websites.
- I will not tell anyone my logins and passwords
- I will only login to the school systems and Mathletics as myself
- I will only edit or delete my own files
- I am aware that some websites and social networks have age restrictions which mean that I should not go on them
- I will only visit internet sites that are appropriate for my age
- I will only communicate with people I know or that a responsible adult has approved
- I will only send polite and friendly messages
- I will not open an attachment, or download a file, unless I have been given permission by an adult
- I will not send/ post photos or videos on the internet unless a trusted adult has given permission
- I will not tell anyone my home address, phone number, give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- If I see anything I am unhappy with or I receive a message I do not like, I will show a trusted adult.

My name: . . . . . Date: . . . . . .

Online safety incident report form

Details of incident

Date happened:

Time:

Name of person reporting incident:

If not reported, how was the incident identified?

Where did the incident occur?

□ In school □ Outside school

Who was involved in the incident?

□ child/young person □ staff member □ other (please specify

Type of incident:

□ bullying or harassment (cyber bullying)

□ deliberately bypassing security or access

□ hacking or virus propagation

□ racist, sexist, homophobic, religious hate material

□ terrorist material

□ drug/bomb making material

□ child abuse images

□ online gambling

□ soft core pornographic material

□ illegal hard core pornographic material

□ other (please specify) _____

Description of incident

Nature of incident

Did the incident involve material being; □ created □ viewed □ printed □ shown to others □ sent to others Could the incident be considered as; □ harassment □ grooming □ cyber bullying □ breach of AUP

Action taken

Staff (includes all paid staff, volunteers, governors, students, casual workers, temporary or supply staff) □ incident reported to head teacher/senior manager □ advice sought from Safeguarding and Social Care/ LADO □ referral made to Safeguarding and Social Care/LADO □ incident reported to police □ incident reported to Internet Watch Foundation □ disciplinary action taken □ online safety/ staff code of conduct policies to be reviewed/amended **Please detail any specific action taken (ie: removal of equipment)** **Child/young person**

□ incident reported to head teacher/senior manager

□ advice sought from Safeguarding and Social Care

□ referral made to Safeguarding and Social Care

□ incident reported to police

□ incident reported to social networking site

□ child's parents informed

□ child/young person spoken to

□ online safety policy to be reviewed/amended

Outcome of incident/investigation

Signature: _____ **Date:_____**