Online E-Safety Policy

Date of Issue: April 2016
Review Date: April 2017

Approved by the Full Governing Body
on 15th June 2016

Audience: Staff/Governors/Public

Frequency of Review: Annually

Postholder responsible for Review: ICT co-ordinator

Recommended associated documents:

Computing Policy including Information Systems.

Social Networking and Cyber Bullying Policy

Safeguarding policy

Gorsemoor Primary School

Online E-Safety Policy

April 2016

For the purpose of this policy E-Safety refers to all Online Safety.

E-safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and ICT environment for Gorsemoor Primary School.

"As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the Internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal.
"To ignore e-safety issues when implementing the requirements of Every Child Matters could ultimately lead to significant gaps in child protection policies, leaving children and young people vulnerable."
From: Safeguarding Children in a Digital World. BECTA 2006

Our e-safety Policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors.
The school's e-safety coordinator is Deborah Le Chevalier
The e-Safety Governor is Mr Arm
The e-safety Policy and its implementation shall be reviewed annually

1.0 Roles and Responsibilities

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. The role of the E-Safety Governor will include:

Regular meetings with the e-Safety Co-ordinator / Officer.
Regular monitoring of e-safety incident logs.
Reporting to relevant Governors committee / meeting.

Headteacher and Senior Leaders:

The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the e-Safety Co-ordinator.

- The Headteacher / Senior Leaders are responsible for ensuring that the e-safety
- Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher and Deputy Head should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The e-safety co-ordinator:

- Takes day-to day-responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority.
- Liaises with school ICT technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Meets regularly with E-Safety Governor to discuss current issues, review incident logs.
- Attends relevant meetings.

Teaching and Support Staff:

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current *school / academy* e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement
- they report any suspected misuse or problem to the Headteacher; E-Safety Coordinator for investigation.
- all digital communications with students / pupils / parents / carers should be on a professional level *and only carried out using official school systems*
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the e-safety and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- *in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*

Students and Pupils

- **are responsible for using the *school* digital technology systems in accordance with the Pupil Acceptable Use Policy**
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the *school's* E-Safety Policy covers their actions out of school, if related to their membership of the school.

2.0 Teaching and Learning

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

- The school Internet access will be designed expressly for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- As part of the new ICT (computing) curriculum, all year groups have digital literacy units that focus on different elements of staying safe on line. These units include topics from how to use a search engine, our digital footprint and cyber bullying.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- When children are directed to websites as part of home learning they will have been
- checked for appropriateness by the teacher setting the learning.

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society. We also measure and assess the impact regularly through meetings with our SEND co-ordinator and individual teachers to ensure all children have equal access to succeeding in this subject.

3.0 Authorised Internet Access

By explicitly authorising use of the school's Internet access pupils, staff, governors and parents are provided with information relating to e-safety and agree to its use:

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff and visitors (making use of access to the computers / internet) must read and sign the 'Acceptable ICT User Agreement' before using any school
- ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access and asked to sign and return a consent form for pupil access.
- Only authorised equipment, software and Internet access can be used within the school.

4.0 Technical Infrastructure and Monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by Mr Richardson who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The administrator passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher and kept in a secure place. More detail regards to the use of passwords, USB pens and encryption of data can be found in the school's ICT and Computing Policy.
- Mr Richardson is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- The school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc)
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place (to be described) for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (eg. trainee teachers, supply teachers, visitors) onto the school systems.

- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.

5.0 World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Headteacher, by recording the incident in an e-Safety Log, which will be stored in the Headteacher's office with other safeguarding materials. The e-Safety Log will be reviewed termly by the e-Safety Co-ordinator.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- The school will work in partnership with the Local Authority to ensure filtering systems are as effective as possible.

6.0 E-mail

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:

- Pupils may only use approved e-mail accounts on the school system.
- 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.
- Pupils may not use personal email accounts at school. Pupils are provided with an individual email address identified by a unique, but anonymous, username.
- E-mail sent to external organisations should be written carefully within the bounds of the professional code of conduct.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

7.0 Social Networking

The school holds a separate Social Networking Policy (see Appendix 5) The following is a summary of the key points.

Social networking Internet sites (such as, MySpace, Facebook, Instagram) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.
- Staff will be provided with the detailed Social Networking Policy (see appendix 5) and must adhere to the code of conduct guidelines set out within it.
- Staff are not to add 'friends' on their social networking sites who are pupils or parents of pupils at the school.
- Pupils will be advised, through the teaching of Digital Literacy units of work in each year group and regular assemblies, never to give out personal details of any kind that may identify
- themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

See also Appendix 5

8.0 Mobile Phones and Tablet Devices

The school holds a separate Mobile Technologies Policy (see Appendix 6). The following is a summary of the key points.

Many new mobile phones and tablets have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils by permission of the Headteacher can bring mobile phones / tablets onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into the school office at 8:45 and collected at the end of the day.
- The sending of abusive or inappropriate text messages is forbidden.

- Staff should always use school phone to contact parents.
- Staff, including students and visitors, are not permitted to access or use their mobile phones within the classroom whilst children are present. They must be kept out of sight.
- Staff may use their mobile phones in the staffroom during the lunch period.
- Staff must not use mobile phones or personal i-pads / tablets to take images or videos of children in school or when out on educational day visits or residential visits.
- Parents cannot use mobile phones on school trips to take pictures of the children.
- School iPads / tablets, used by staff within Early Years for assessment purposes, must be passcode protected.

See also the Mobile Technologies Policy in Appendix 6

9.0 Digital/Video Cameras

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

- Pupils will not use digital cameras or video equipment at school unless specifically
- authorised by staff.
- Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.
- Parents will not use digital cameras, mobile phones or video equipment at school unless specifically authorised by staff.
- Staff will only use school memory cards within digital cameras to take images / videos of children.
- The Headteacher or nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner

10.0. 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.

11.0 Published Content and the School Website

The school website is a valuable source of information for parents and potential parents. Contact details on the Website will be the school address, e-mail and telephone number.

- Staff and pupils' personal information will not be published.

- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Website, particularly in association with photographs.
- Consent from parents 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.
- Parents may upload pictures of their own child only onto social networking sites. If the picture includes another child / children then it is their responsibility to gain permission from that child's parents.
- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

12.0 Assessing Risks

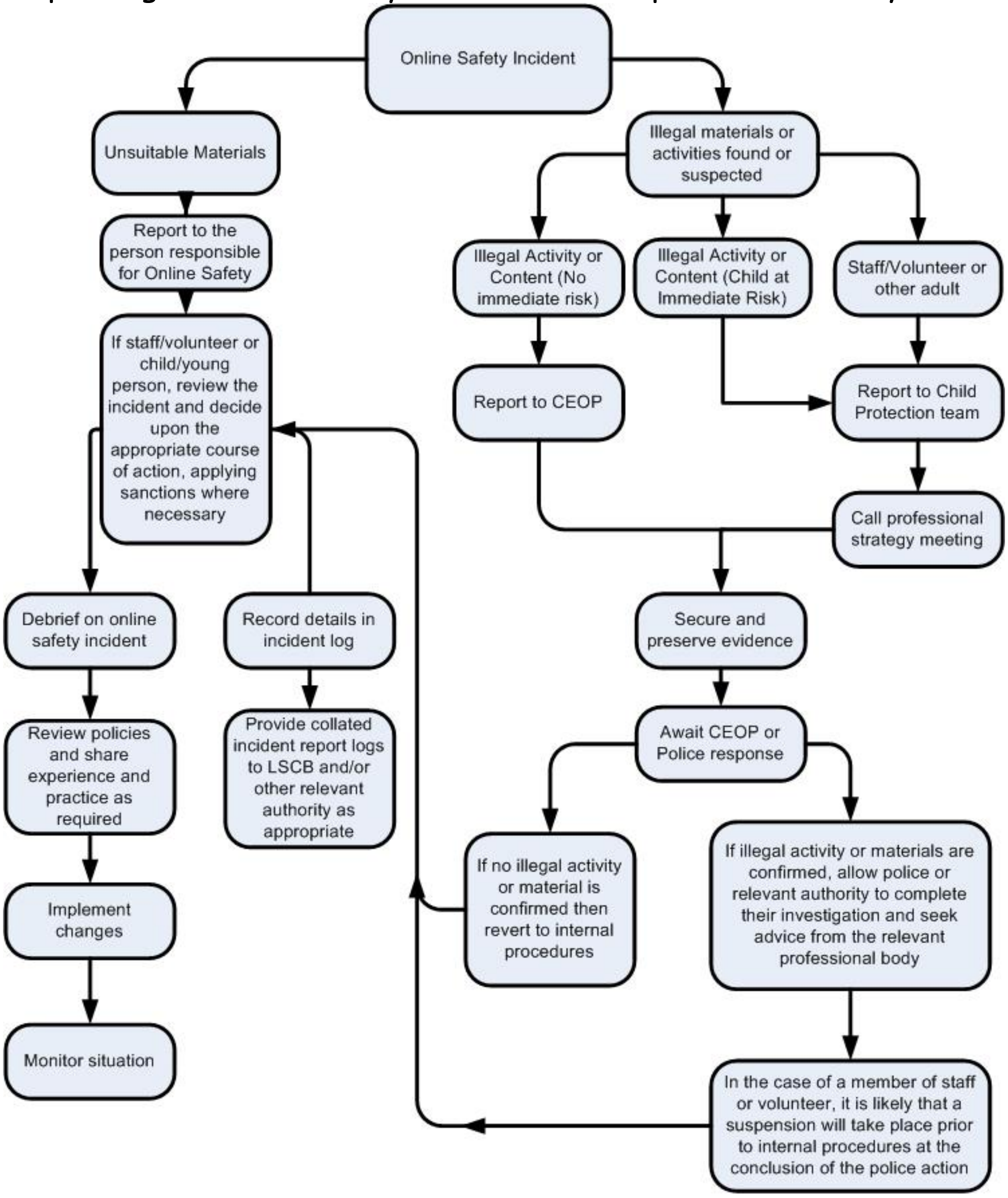
The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

13.0 Responding to incidents of misuse

- Complaints of Internet misuse will be dealt with by a senior member of staff. Technician, Stephan Richardson, will be responsible for keeping a written log of any incidents flagged up through the school's monitoring software. This will be reviewed and signed weekly by the Head teacher and ICT co-ordinator.
- Any complaint about staff misuse must be referred to the Headteacher
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

13.1 Illegal incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

13.2 Other incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school / academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

14.0 Communication of Policy

Pupils:

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Pupils will be informed when they are in Y2 of the importance of being safe on social
- networking sites such as MSN. This will be strongly reinforced across all year groups during ICT lessons and all year groups look at different areas of safety through the digital literacy lessons.

Staff:

- All staff will be given the School Online and 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.

Parents:

- Parents' attention will be drawn to the School e-safety Policy in newsletters and on the school Website.

Further Resources

We have found these web sites useful for e-safety advice and information.
http://www.gorsemoor.staffs.sch.uk Our school's web site for other policies and school information
http://www.staffsscb.org.uk/ Staffordshire Safeguarding Children Board's site with locally provide information on all aspects of protecting children.
http://www.thinkuknow.co.uk/ Set up by the Police with lots of information for parents and staff including a place to report abuse.
http://www.childnet-int.org/ Non-profit organisation working with others to "help make the Internet a great and safe place for children".

Equalities Statement

Through appropriate treatment of all, Gorsemoor Primary School aims to eliminate unlawful discrimination, prejudice, harassment and stereotyping and strive to maintain policies that comply with current legislation. This applies to all members of the school community – pupils, staff, governors, parents/carers and community members and is based on the School's core values.
During the review of this policy the nine protected characteristics of the Public Sector Equality Duty, i.e. race, disability, religion or belief, sexual orientation, pregnancy, maternity and gender reassignment have been considered.

Gorsemoor Primary school acknowledges the assistance of Sheffield City Council, SWGFL and Kent County Council in providing content for this document.

DATE: April 2016 REVIEW DATE : Spring Term 2017

Appendix 1

Gorsemoor County Primary School

Headteacher: Mrs B S Heath
Tel: (01543) 274788
Fax: (01543) 278623

Gorsemoor Road,
Heath Hayes,
Cannock,
Staffs.
WS12 3TG

E Safety for Pupils.

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will only use the computers for school work and homework;
- I will ask permission from a member of staff before using the Internet. But an adult must be present;
- I will not access other people's files;
- I will only access e-mail with my own login and password using Outlook Express
- I will only e-mail people I know, or my teacher has approved;
- I will not open an attachment that may be suspicious, and I will alert an adult.
- The messages I send will be polite and responsible; I understand that Mrs Heath will be notified of any unsuitable language that I might send. This will lead to my parents being informed.
- I will not give my home address or telephone number, or visit a chat room or arrange to meet someone, unless my parent, carer or teacher has given permission;
- I will report any unpleasant material or messages sent to me. I understand my report would be confidential and would help protect other pupils and myself;
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- I will not use my mobile phone to E bully anyone inside or out of school.
- I will hand my mobile phone into the office for security during the school day.
- I will not use my mobile phone to take images of teachers and pupils unless I have permission.
- I will not publish any images of other pupils or staff that may cause hurt.

Name of pupil. Printed clearly ____

Signed/ Pupil ____________________________________Class ____________________________

Signed /Parent or Guardian _________________________ Date_________________________________

Appendix 2 Staff code of Conduct.

Gorsemoor County Primary School

Headteacher: Mrs B S Heath
Tel: (01543) 274788
Fax: (01543) 278623

Gorsemoor Road,
Heath Hayes,
Cannock,
Staffs.
WS12 3TG

An Internet E Safety and E-Mail Code of Conduct for Staff.

The computer system is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties - the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Staff and students requesting Internet access should sign a copy of this Acceptable Internet Use Statement and return it to the ICT Co-ordinator for approval.

- All Internet activity should be appropriate to staff professional activity or the student's education;
- Access should only be made via the authorised account and password, which should not be made available to any other person;
- Passwords must be secure ref appendix 16 in ICT policy
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden;
- Users are responsible for all e-mail sent and for contacts made that may result in inappropriate e-mail being received;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Copyright of materials must be respected;
- Posting anonymous messages and forwarding chain letters is forbidden As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- It is vital to be aware that posting unsuitable images on social network spaces and unsuitable messages may cause personal embarrassment and may infringe professional integrity of yourself and colleagues.

Full Name : ______________________________ Post :_________________

Signed : _____________________________________ Date: ________

Appendix 3

Photography and Video Consent.

Dear Parent/ Guardian

At Gorsemoor Primary we follow strict guidelines to protect your child on our school website, plasma screen, newsletters and in the local press. However, because we are proud of what our children do, we also want to be able to celebrate and share your child's achievements in class work, drama and sport both here in school and with the wider community. This also includes having photographs on display in the classroom of your child's achievements

Our code of practice is as follows:

- We will never use photographs if you as a Parent/Guardian do not agree to our policy.
- We will always do our best to ensure that single photographs of children are not published.
- We will not use photographs of pupils in PE clothes or swimwear other than for instructional purposes where we demonstrate an activity to the rest of the class or teachers for instructional use.
- We will not reveal the child's surname, age, home address or telephone number.
- We will try and use rear views of heads if parents so request us to do so.
- We will not use close up images of pupils on the internet or online.

By reading and understanding our code of practice, we hope that you will agree to our using your child's photograph. If we do not hear from you we will include your child in our positive response list. However, if you have any concerns please come and discuss these with your child's class teacher.

Yours Sincerely.

B S Heath

Acting Headteacher.

Appendix 4

Letter template for Misuse of Internet, Email or Computer Facilities at Gorsemoor.

Please copy onto school headed paper, add a date and keep a copy in the child's classroom file.

Dear Parent,

I regret to have to inform you that your child_______________ has been found to have misused the trust placed upon them in using the school computer network.

You will recall that we request that you and your child sign an Internet and email code of conduct at the start of every academic year.

Can we please ask that you discuss the matter with your child? In this way we can ensure that every child at Gorsemoor uses the school network in a safe and caring manner so as not to bring themselves or any other pupil or member of staff into danger, harm or hurt.

We thank you for your cooperation in this matter.

Yours Sincerely

Mrs B. S. Heath

Appendix 5

Social Networking and Cyber Bullying Policy

Date of Issue: April 2016
Review Date: April 2017

Approved by the Full Governing Body
on 15th June 2016

Recommended associated documents:

Computing Policy including Information Systems.

Online Safety Policy

Audience: Staff/Governors/Public

Frequency of Review: Annually

Postholder responsible for Review: ICT co-ordinator

Code of Practice for Employees in the use of Social Networking Sites and Electronic Media.

1.0 Protecting yourself and others in the use of Social Networking Sites and electronic media.

This code of practice provides employees with guidance to ensure they are taking necessary steps to protect themselves and others against Cyber bullying.
It also provides employees with practical guidance on how they can ensure that their conduct in relation to social networking sites and electronic media is in accordance with the code of conduct for all Local Government employees as interpreted by Staffordshire County Council in relation to social networking sites and electronic media.

2.0 Cyber Bullying

Definition: Cyber bullying is the use of Information and Communications Technology; particularly mobile phones and internet, deliberately to upset someone else.
(Cyber bullying: Guidance issued by the DCSF 2007)

Staffordshire County Council supports the view that cyber bullying represents a cruel, dangerous and inescapable form of bullying that causes humiliation, stress and trauma to its victims, and so believes that cyber bullying is not acceptable and will not be tolerated.

Staffordshire County Council is committed to the view that cyber bullying is never acceptable and is not tolerated.

3.0 Legislation

Although bulling is not a specific criminal offence, criminal law exists to prevent certain behaviours. These behaviours may constitute harassment, or cause fear of violence. Sending indecent, grossly offensive or threatening letters, electronic communications or other articles to another person is illegal.
Other legislation protects against the publication of obscene articles or data (e.g. over a school intranet), hacking into someone else's computer, invading their privacy, damaging their reputation or engaging in anti-social acts.

4.0 **Protecting yourself against Cyber Bullying**

There are simple measures that you can take to safeguard against cyber bullying.

- Being careful about personal information and images posted on the internet.
- Not leaving your mobile phone or personal computer around for others to gain access to or leaving details on view when left unattended.
- Choosing hard to guess passwords and not letting anyone know them
- Being aware of the risks of giving your mobile number or personal email address to others
- Making use of blocking facilities made available by website and service providers
- Not replying or retaliating to bullying messages
- Saving evidence of offending messages
- Making sure you inform others of any mobile phone or online bullying or harassment in accordance with relevant policies.

5.0 What action can you take

You can report any incidents in relation to cyber bullying in the work environment in accordance with county council's Harassment and Bullying policy. If you make a complaint you have a right to have it investigated, and to seek assistance from managers, colleagues or trade unions in doing so.

Cyber bullying complaints will be investigated to obtain any evidence available and you can support this process by:

- Logging any incidents
- Noting the dates, times and content of messages and, where possible, the sender's identity or web address.

Taking an accurate copy of the whole web page address, for example, helps service providers locate offending material. Such evidence may be required also to show to those who need to know, including police. Saving evidence of texts and images on the device can be useful. It is important they are not deleted.

In the non-work environment it may be appropriate to report incidents of cyber bullying direct to an internet service provider or mobile phone company. Content may be blocked and / or removed if it is illegal or breaks providers own terms and conditions. Some providers issue conduct warnings to users and are able to delete the accounts of those who have broken the rules.

Some cases may raise allegations against staff and in such cases, immediate referral should be made via the First Response Team to one of the Local Authority Designated Officers who will provide initial advice and guidance.

6.0 Code of Conduct

As a Condition of Service, all employees are expected to maintain conduct of the highest standard such that public confidence in their integrity is maintained.

This employment obligation is also reinforced, in relation to certain posts, by a duty to comply with external standards – as applies, for example, to Social Workers under the GSCC Codes of Conduct, or the requirements of professional bodies such as the Law Society.

You are reminded that care should be taken with the use of personal social networking sites to ensure the integrity of the county council is maintained and to this end you should ensure that you take account of the expectations of all employees with regard to all aspects of the employees code of conduct when posting information, messages, pictures or video footage these may include.

1. Bringing the county council into disrepute
2. Confidentiality
3. Policy restrictions

Care should be taken of the legislative measures that already exist e.g. Invasion of privacy, harassment.

7.0 Safeguarding

In order to safeguard yourself and potentially vulnerable adults and young people who you may work with you should ensure that your behaviour with regard to social networking sites is consistent with the standards of behaviour expected in normal day to day interactions with vulnerable adults and young people.

Communication that is undertaken via social networking sites is comparable to 'one to one' interaction in other contexts and individuals should avoid any activity which would lead any reasonable person to question their motivation and intentions.

You are reminded that it is expected that you:

a) Always act in such a way as to promote and safeguard the wellbeing and interests of service users and colleagues.
b) Take all reasonable steps to ensure the relationships with service users and colleagues are such that there can be no suggestion of impropriety whether by word or action
c) Develop a friendly relationship between employee and service users, with clear boundaries. It is deemed an abuse of that professional relationship for an employee:
    - To enter into an improper relationship with a service user
    - To show favour towards a particular service user
    - To act in a threatening or aggressive manner or to use foul, abusive or profane language
    - To endeavour to exert an undue influence with regard to personal attitudes, opinions or behaviour which is in no way connected to the work of the Service.

d) Take all reasonable steps to ensure no action or omission on your part or within your sphere of influence is detrimental to the condition or safety of service users

In order to preserve these standards of behaviour it is recommended that you decline any request from an existing or previous service user to be a 'friend' on your social networking site. Parents of children at school should not be 'friends' on your social networking site.
It is inappropriate to request contact with an existing or previous user of the service via this medium or any other form of electronic medium.
It is acknowledges that you may accept a service user as a 'friend' unintentionally and where this occurs you are advised to ensure that you remove this access as soon as you become aware of their status. You should do this in a way that does not jeopardise your professional relationship and should inform you Line Manager, is any significant conversation or activity occurs.
All employees are advised to ensure that when setting up social networking sites they should make full use of the range of tools which enable access to personal information to be restricted.

Appendix 6

Mobile Technologies including Bring Your Own Device (BYOD) Policy

Date of Issue: April 2016
Review Date: April 2017

Approved by the Full Governing Body
on 15th June 2016

Recommended associated documents:

Computing Policy including Information Systems.

Online Safety Policy

Safeguarding Policy

Audience: Staff/Governors/Public

Frequency of Review: Annually

Postholder responsible for Review: ICT co-ordinator

Rationale

Mobile technology devices may be defined as a school owned/provided **or** privately owned smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

The absolute key to considering the use of mobile technologies is that the pupils / students, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school owned/provided or personally owned.

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen student learning, but they can also develop digital literacy, fluency and citizenship in students that will prepare them for the high tech world in which they will live, learn and work.

For further reading, please refer to "Bring your own device: a guide for schools" by Alberta Education available at: http://education.alberta.ca/admin/technology/research.aspx and to the "NEN Technical Strategy Guidance Note 5 – Bring your own device" - http://www.nen.gov.uk/bring-your-own-device-byod/

1.1.1 Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to your school network, filtering of personal devices, breakages and insurance, access to devices for all students, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership

Schools may consider implementing the use of mobile technologies as a means of reducing expenditure on school provided devices. However, it is important to remember that the increased network management costs and overheads involved in implementing this properly are likely to counterbalance or outweigh any savings.

The use of mobile technologies brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset. Before the school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

- The school allows:

	1.1.1.1 School Devices			1.1.1.2 Personal Devices		
	School owned and allocated to a single user	School owned for use by multiple users	Authorised device[1]	Pupil/Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes	Yes	Yes
Full network access	*Yes*	*Yes*	*Yes*	No	No	No
Internet only				Yes	Yes	Yes
No network access						

- The school has provided technical solutions for the safe use of mobile technology for school devices/personal devices
    - All school devices are controlled though the use of Mobile Device Management software
    - Appropriate access control is applied to all mobile devices according to the requirements of the user
    - The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
    - For all mobile technologies connected to the school Wi-Fi, filtering will be applied to the internet connection and attempts to bypass this are not permitted
    - Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user.
    - All school devices are subject to routine monitoring
    - Pro-active monitoring has been implemented to monitor activity

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school

- When personal devices are permitted:
  - All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access
  - Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school
  - The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)
  - The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues
  - The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security
  - The school is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues
  - The school will provide a safe place to keep devices in during the day when they are not in use.
- Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition;
  - Devices may not be used in tests or exams
  - Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements
  - Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network
  - Users are responsible for charging their own devices and for protecting and looking after their devices while in school
  - Personal devices should be charged before being brought to school as the charging of personal devices is not permitted during the school day

- Devices must be in silent mode on the school site and on school buses
- School devices are provided to support learning. It is expected that pupils/students will bring devices to school as required.
- Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- The changing of settings (exceptions include personal settings such as font size, brightness, etc…) that would stop the device working as it was originally set up and intended to work is not permitted
- The software / apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps
- The school will ensure that school devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to students on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.
- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- Images must be taken in accordance with the school's Digital Images Policy. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately and are not to be taken off school premises.
- Devices may be used in lessons in accordance with teacher direction
- Staff owned devices should not be used for personal purposes during teaching sessions.
- Printing from personal devices will only be carried out under supervision.

Gorsemoor Primary school acknowledges the assistance of SWGFL in providing content for this document.