Barlby Bridge Primary School

Online Policy (formerly e-safety policy)

This policy has been written based on NYCC Online Safety Guidance for Schools and Settings in North Yorkshire document (October 2016).

January 2017

This policy is for all members of the school community (including staff, pupils, governors, volunteers, parents/ carers and visitors) who have access to school IT systems and use of personal technologies whilst on school premises or engaged in school activities off site.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school will deal with such incidents within the procedures set out in the online policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that takes place out of school.

Today's children's daily use of the Internet and digital technologies represents a seamless extension of their physical world as well as their emotional lives and their development. As online content, social networks and instant messaging converge with mobile technology to produce lives which are always 'on', any line which may have existed between being online and offline is disintegrating.

For the majority of children and young people, internet technologies are not a 'new thing' as they are for many adults. They are simply another part of the world they have grown up with. Despite this, all who provide services and support to children and young people must recognise that for many children technology is now an important, if not the main way, in which they send and receive information, access entertainment and, perhaps most importantly, communicate with people.

The online safety policy encompasses Internet technologies and electronic communications such as mobile phones. This policy highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experiences.

Our school believe that in order to maximize the opportunities within this technological environment, whilst minimising the potential risks, we must encourage children and young people to develop as responsible online citizens. Children must be taught to recognise their responsibility to keep themselves safe online as well as accepting the responsibility they have to present themselves as positive role models. It is only through the development of a sense of online responsibility that we can ensure the safety and well-being of today's children and young people.

The school has appointed an e–Safety Coordinator.
The e–Safety Policy and its implementation will be reviewed annually.
Our School Policy has been agreed by the Senior Leadership Team and approved by Governors.
The School has appointed a member of the Governing Body to take lead responsibility for e-Safety

The School e-Safety Coordinator is
The School e-Safety Governor is Stephen Walker
Policy approved by Head Teacher: ………………………………………………… Date: ……………
Policy approved by Governing Body: … ………… Date: …………

TEACHING AND LEARNING

Why is Internet use important?
The rapid developments in electronic communications are having many effects on society.

- 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 school's management functions.
- Internet use is a part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for children who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st Century life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely 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?

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

Benefits of using the Internet in education include:
- access to worldwide educational resources including museums and art galleries;
- the possibility of educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- 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 networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- access to learning wherever and whenever convenient.

How can Internet use enhance learning?

Developing effective practice in using the Internet for teaching and learning is essential. Pupils need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught.

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils, provided by a local authority firewall.
- 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. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the 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.

What are the potential risks of internet and social media use?

Keeping Children Safe in Education (Sept 16) states that, "The use of technology has become a significant component of many safeguarding issues. Technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school to protect and educate the whole school in their use of technology and establishes mechanisms to identify, intervene and escalate any incident where appropriate."

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:
- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm
-

Some of the risks users may face include:
- Access to illegal, harmful or inappropriate images or other content (including radicalisation /extremism material and pornography)
- Unauthorised access to, loss of or 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 with and without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/Internet games/ websites
- 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
- Generating large bills through overuse of their mobiles, gaming etc

Roles, Responsibilities and Training

Online safety is everyone's responsibility within school. However, governors have a statutory duty to ensure that online safety procedures remain upto date, are adhered to and monitored. The headteacher is the designated safeguarding lead.

Staff receive face to face training once every two years. Workshops are also offered to parents.

Pupils are taught specifically about how to keep themselves safe when on the internet through a well-planned curriculum that is age appropriate based on the needs of the pupils.

Online safety education will be provided in the following ways:
- A planned online safety programme is provided as part of the PSHE and assembly programme and is regularly revisited in Computing and other lessons across the curriculum – this programme covers both the use of ICT and new technologies in school and outside of school.
- A range of safeguarding issues are considered as part of the online safety education: keeping their personal information private, healthy relationships on and off line, grooming, sending inappropriate images and the consequences of this, gaming, gambling, radicalisation and how to recognise the signs and keep themselves safe
- Pupils are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- Pupils are helped to understand the need for the Pupil AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

See appendix 1- Roles and responsibilities

MANAGING INFORMATION SERVICES TO MINIMISE RISK
This section of the policy contains information about how we will manage users and sets out what we consider to be acceptable uses for a range of technologies.

Maintaining ICT system security.

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Use of data storage facilities by pupils within school is prohibited to protect against virus transfer.
- Files held on the school's network will be regularly checked.
- The ICT Subject Leader/ Network Manager will ensure that the system has the capacity to take increased traffic caused by Internet use.
- See Appendix 2 showing which technologies are permitted for use by staff and pupils at Longman's Hill School
-

Managing Filtering of Inappropriate Content

- The school will work in partnership with parents and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- A firewall which effectively filters unsuitable websites.
- In the unlikely event that staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Subject Leader. Children will be taught to turn off the screen only if they come across unsuitable sites.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be referred to the IWF Internet Watch Foundation) or CEOP (Child Exploitation and Online Protection).
- The headteacher will carry out random checks to see which sites have been accessed/ attempted to be accessed.

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 by staff during lessons. The sending of abusive or inappropriate text messages is forbidden.
- Instant messaging will not be permitted.

How should personal data be protected?

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

Appropriate use of websites
- All staff and pupils will be expected to sign and adhere to an 'Acceptable Use Policy' – see appendices 3 and 4

- Staff will be aware of which activity is illegal and therefore obviously banned and possibly lead to criminal prosecution. They will also be aware of other activities which may generally be legal but which would be inappropriate in a school context. See Appendix 5- Unsuitable / inappropriate Activities on the internet.
- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use; processes are in place for dealing with any unsuitable material that is found in Internet searches – children will turn off screen and inform adult. Staff will notify safeguarding lead immediately who will contact Schools ICT for further support in filtering / blocking the content or site.
- "Open" searches (e.g. "find images/ information on...") are discouraged when working with pupils who may misinterpret information
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff. Parents will be advised to supervise any further research
- All users must observe copyright of materials published on the Internet
- Teachers will carry out a risk assessment regarding which pupils are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the pupils on the internet by the member of staff setting the task. All staff are aware that if they pass pupils working on the internet that they have a role in checking what is being viewed.
- All internet use at school is monitored and logged; staff and pupils are made aware of this. The school only allows the ICT technician and headteacher to access these logs.

Appropriate use of mobile phones
- Staff should not use personal mobile devices to contact parents / carers and under no circumstances should a pupil or parents/carers be given a member of staffs personal mobile number
- Staff should not use personal mobile phones in school during working hours when in contact with children
- Visitors will be asked not to use their mobile phone whilst on site with any pupils present due to all mobile phones containing a camera
- Pupils are not permitted to have mobile phones in school except where agreed for exceptional parents with parents in advance. In such cases, pupils must hand the phone to the school office at the start of the day where it will remain until the end of the school day.

Appropriate use of E-mail

- Pupils **do not** have access to their own school-based email account.
- Any e mails sent by children will be directly linked to curriculum learning and will use the school e mail address. Teachers will be responsible for checking the content of any e mails, prior to sending.
- Children will not divulge ANY personal information in e mails which may result in them being identified. First names only will be used.
- The forwarding of chain messages is not permitted.
- Digital communications by staff with parents / carers (e-mail, online chat, VLE, voice etc.) should be on a professional level and only carried out using official school systems
- The school's e-mail service should be accessed via the provided web-based interface by default
- Under no circumstances should staff contact pupils, parents/carers or conduct any school business using personal e-mail addresses
- School e-mail is not to be used for personal use
- All staff should be aware that emails can be part of Freedom of Information requests so all correspondence needs to be professional, courteous and respectful
- If confidential information / information under the data protection act is being sent by email it must be sent through the secure email system

Appropriate use of Social Media

- The school will block access to social networking sites. However, pupils will be taught about online safety when using social networking sites
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended or e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. House number, street name or school.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.
- Students should be advised not to publish specific and detailed private thoughts.

- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for children to use on a personal basis.
- Staff should not access social networking sites on school equipment in school or at home that have not been pre-approved by the school
- Staff users should not refer to any member of staff, pupils, parents/carers, the school or any other member of the school community on any social networking site or blog in a derogatory way
- Pupils/Parents/carers should be aware the school will investigate misuse of social networking if it impacts on the well-being of other pupils or members of the school community
- Parents / carers and pupils will be informed that they do not use social media to criticise or make inappropriate comments about the school, an individual member of staff or another pupil as making defamatory comments online has exactly the same legal consequences as if they are made directly to someone else. Similarly threats of violence can lead to criminal proceedings under the Malicious Communications Act. If as a parent/ carer they have any concerns about anything which happens in schools then they will be asked to contact the school directly
- If inappropriate comments are placed on social networking sites about the school or school staff then advice would be sought from the relevant agencies, including the police if necessary

School Facebook Page

Social media can be a fantastic way for schools to communicate with the wider community. Maintaining an online presence is vital, not only in terms of keeping our school community up to date with what's happening in school, but also in terms of attracting potential enrolment.

Appropriate use of the school's Facebook Page

- To publicise school events and increase awareness about school fundraising. Having a school website is an essential part of this, but web users must specifically visit the school website regularly to receive the information. By using Facebook the information is more likely to reach parents and carers and the wider school community directly as it is being fed into their personal news feeds.
- To highlight positive school achievements in a forum where they can be shared by the school community.
- To make school announcements (e.g. school closure due to snow).
- To facilitate communication and networking opportunities between parents, especially new or prospective parents.
- To maintain contact with past parents and past pupils.
- Users should not post anything on the page that could be deemed as offensive – inappropriate or harmful comments/content will be removed immediately.
- Users should not engage in giving negative feedback on Facebook, it is more appropriate to deal with the school directly on such matters.
- Users will not mention individual staff members in a negative light.
- Users should not ask to become "friends" with staff as failure to respond may cause offence.
- Any comments and requests to tag or post photographs will be reviewed by the page administrator.
- The sanction for any user breaking any of the above rules is removal from the Facebook group.
- Facebook lists a minimum age requirement of 13 and all parents are reminded that children under the age of 13 should not be on Facebook.
-

Appropriate use of digital images and work, including those of pupils.

- Images which include pupils will be selected carefully and only those children whose written parental permission has been sought will be used. This list is held in the school office.
- Pupils' full names will not be used on the Website when associated with photographs, or in any way which may be to the detriment of pupils.
- Pupil photographs will immediately be removed from the school Website upon request from parents, or other appropriate request.
- Under no circumstances should images be taken by staff or Governors using privately owned equipment
- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file
- Visitors / contractors will be asked not to use their mobile phone whilst on site with any pupils presence due to all mobile phones containing a camera
- Whilst parents/ carers can take images at a school event e.g school play, sports day they must not be used on social networking sites and parents are reminded of this at each event. School reserves the right to ask parents to remove images if found on social media sites which contain images of children other than their own.

Appropriate use of Removable Data Storage Devices
- Any memory / removable data devices/ USB pens used by staff must be encrypted
- Any information that is on removable data storage device for school use should not be transferred onto any personal devices, in particular any information that is covered by the data protection act and could lead to an individual being identified
- All files downloaded from the Internet, received via e-mail or provided on removable media (e.g. CD, DVD, USB flash drive, memory cards etc.) must be checked for viruses using school provided anti-virus software before run, opened or copied/moved on to local/network hard disks
- Pupils should not bring their own removable data storage devices into school for use on school equipment.
- Staff are encouraged to use 'RM Portico' as a secure way to access files stored on the school server from off site.

Appropriate use of School ICT Equipment
- Privately owned ICT equipment should never be connected to the school's network and no personally owned applications or software packages should be installed on to school ICT equipment
- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted
- If staff are working on confidential documents, all should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access

Managing Videoconferencing

- At present, the school does not have any video conferencing equipment and does make use of web cams or any similar technologies.

Managing Content on the School Website

- The point of contact on the Web site will be the school address, school e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure content is accurate and appropriate on all pages directly related to the day-to-day workings of the school.
- The Website complies with the Local Authority guidelines for website content.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

MANAGING REPORTS OF MISUSE

Incident Reporting
Any online safety incidents must immediately be reported to the designated safeguarding lead (headteacher) who will investigate further and notify Schools ICT.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse.

Appendix 6 and 7 outline the responses that will be made to any apparent or actual incidents of misuse from pupils and staff. If any apparent or actual, misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity or materials, the headteacher will liaise with the Police and seek advice. Actions will be followed in accordance with advice, in particular with regards to the preservation of evidence. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

When considering an online safety incident involving a pupil(s) a school does need to take into account the nature of the incident, the age of the child and if there is a need to involve any partner agencies.
- Sanctions available include:
  - interview/counselling by senior member of staff/class teacher/teaching assistants;

- informing parents or carers;
- removal of Internet or computer access for a period, which could prevent access to school work held on the system.

The vulnerability checklist can provide a wider understanding of a range of risk factors that may be impacting on children and young people.
http://www.safeguardingchildren.co.uk/vcl-v3
The Local Safeguarding board has a number of practice guides for professionals which contain information and referral pathways, the aspects that could be highlighted from an online safety incident include:

- Prevent Practice Guide - Working with Individuals Vulnerable to Extremism
http://www.safeguardingchildren.co.uk/prevent-practice-guidance?v=preview
- Child Sexual Exploitation - http://www.safeguardingchildren.co.uk/professionals/cse

Professionals in all agencies have a responsibility to refer a child to Children's Social Care (part of the Children and Families Service)/Disabled Children's Service when it is believed or suspected that a child:

- Has suffered significant harm and /or;
- Is likely to suffer significant harm and/or;
- Has developmental and welfare needs which are likely only to be met through provision of family support services (with agreement of the child's parent).

- **Contact details:** By Phone: 01609 780780 Email:social.care@northyorks.gov.uk

POLICY DECISIONS

How will Internet access be authorised?

- All staff and pupils will initially be granted Internet access.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form.
- Guidelines relating to Internet safety are visible from all machines with Internet access, throughout the school.

How will the risks be assessed?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material.
- However, due to the global and linked nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences resulting from Internet use.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Headteacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

COMMUNICATION OF THIS POLICY

How will the policy be introduced to pupils?

- Rules for Internet access will be posted on or near all computer systems with Internet access.
- An e-safety training programme will be introduced to raise the awareness and importance of safe and responsible Internet use both at school and home.
- Internet safety guidelines will be prominently linked from the school website (Children's Learning Zone) Internet sites.
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use will accompany Internet access.

How will the policy be discussed with staff?

- All staff will be given the School e-Safety Policy and its application and importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff should only operate monitoring procedures on instruction from the Leadership Team.
- Staff training in safe and responsible Internet use, and on the school e-Safety Policy will be provided as required.

How will the policy be discussed with parents?

- Parents' attention will be drawn to the School e-Safety Policy in newsletters and on the school website.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This may include leaflet distributions, demonstrations, practical sessions and suggestions for safe Internet use at home.

Appendix 1
Roles and Responsibilities

Governors:
Governors are responsible for the approval of the online safety policy, ensuring it is disseminated to the wider school community and for reviewing the effectiveness of the policy. There is a named member of the Governing Body who takes on the role of online safety governor who has accessed training about online safety. The role of the governing body does include:
- Ensuring that the statutory requirements of Keeping Children Safe in Education (Sep 2016) are complied with. In relation to online safety this includes:
  - Ensuring that as part of the requirement for staff to undergo regularly updated safeguarding training and the requirement to ensure children are taught about safeguarding, including online that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach
  - Ensuring that pupils are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum. This may include covering relevant issues through PSHE
- As schools increasingly work online it is essential that children are safeguarded from potentially harmful and inappropriate online material. A school needs to ensure the appropriateness of any filters, monitoring and security systems which will be informed in part by the risk assessment required by the Prevent Duty to ensure that children are safe from terrorist and extremist material whilst accessing the material in school, including by establishing appropriate levels of filtering but being careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding'.
- Regular monitoring of online safety incident logs and responding appropriately to the identified needs
- Ensure the company who is hosting the schools website has enough security in place so it cannot be inappropriately accessed and to have an action plan if it is 'hacked' e.g who regular checks the website including during school holidays, who is the key contact if the website is hacked

Roles & Responsibilities of the Headteacher:
- Supporting the Governors comply with the online safety aspects of the Keeping Children Safe in Education, September 2016 documentation
- The safety (including online safety) of all members of the school community.
- Effective and regular training about online safety is provided for the whole school community and a log is kept of the staff who complete the training

- Governors are invited to take part in online safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, online safety education, health and safety or child protection.
- Effective communication with parents/ carers about safe practices when using online technology's and support them in talking to their children about these issues
- Effective filtering, monitoring and security systems are set up
- There are effective procedures in place the event of an online safety allegation which are known and understood by all members of staff
- Establishing and reviewing the school online safety policy and documents and making them available on the school website

The school's Designated Safeguarding Lead is trained in online safety issues and is aware of the potential for serious child protection issues that could arise through the use of ICT.

Roles & Responsibilities of a named member of the Senior Leadership Team:
- Liaising with staff, ICT Technical staff, online safety governor, SLT and partner agencies on all issues related to online safety
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Providing training and advice for staff and keeping a log of staff who complete training about online issues
- Keep a log of staff, pupils and families who have signed the Acceptable Use Policy (AUP) for the safe use of technology
- Receive and respond to reports of online safety incidents and creates a log of incidents and outcomes to inform future online safety developments
- Co-ordinating and reviewing online safety education programme in school (or working in partnership with the Personal, Social, Health, Education (PSHE) and/ or Computing lead).

Roles & Responsibilities of the ICT technician:
- The school's ICT infrastructure is secure and meets requirements for filtering and monitoring
- The school's website is kept secure from 'hacking' and there is an action plan in place if it is hacked
- The school's password policy is adhered to
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- Keeps up to date with online safety technical information
- The use of the school's ICT infrastructure (network, remote access, e-mail, VLE etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the named SLT for action.

Roles & Responsibilities of all staff:
In addition to the elements covered in the Staff Acceptable Use Policy (AUP), all staff are responsible for ensuring that:
- They have an up to date awareness of online safety matters and of the schools current online safety policy and practices
- They attend the training provided by the school about online safety and all new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy, Acceptable Usage and Child Protection Policies.
- They have read, understood and signed the school Staff Acceptable Usage Policy (AUP)
- They do not 'be-friend' any pupil or pupil family member on social media in a social context whilst the pupil is at the school
- Online safety issues are embedded in all aspects of the curriculum and other school activities
- Pupils understand and follow the school's online safety and acceptable usage policies
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended school activities
- In lessons where Internet use is pre-planned, 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.
- All staff should be aware that emails can be part of Freedom of Information requests so all correspondence needs to be professional, courtesy and respectful
- If confidential information / information under the data protection act is being sent by email it must be sent through the secure email system which if provided by Schools ICT would be the Egress system which the schools administration and headteacher have access to but more licenses can be purchased.

Roles & Responsibilities of all pupils
- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Usage Policy, which they will be required to sign before being given access to school systems. Parents/carers will be required to read through and sign alongside their child's signature.

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy also covers their actions out of school, if related to their membership of the school or using equipment provided by the school.

Roles & Responsibilities of all parents/carers:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. Schools will therefore take opportunities to help parents understand these issues. Parents and carers will be responsible for:
- Endorsing (by signature) the Pupil Acceptable Usage Policy and will alongside this sign the Parents Acceptable Usage Policy
- Ensuring that they do not use social media to criticise or make inappropriate comments about the school or an individual member of staff as making defamatory comments online has exactly the same legal consequences as if they are made directly to someone else. Similarly threats of violence can lead to criminal proceedings under the Malicious Communications Act. If as a parent/ carer they have any concerns about anything which happens in schools then please contact the school directly.

Parents and Carers should also be aware of the health effects of children and young people having too much 'screen time'. This can limit the amount of time children are being physically active, reduce the amount of time they are sleeping and could be impacting on their eyesight. A number of systems and apps are available that can limit the screen time for children and young people alongside parents and carers talking to their children about the issues.

Appendix 2
Permitted technologies – staff and pupils

Communication Technologies	Permitted	Permitted at certain times	Permitted for named staff	Not Permitted	Permitted	Permitted at certain times	Allowed with staff permission	Not Permitted
Mobile phones may be brought to school	✓						✓	
Mobile phones used in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Staff contacting a pupil on a				✓				

	1	2	3	4	5	6	7	8
mobile phone								
Taking photographs/film on personal mobile devices / digital camera				✓				✓
Taking photographs/film on school mobile devices / digital camera for school purposes only	✓						✓	
Parent / carer taking photos of a school event on their own device and uploading online with public access				✓				✓
Use of personal tablets/ laptops ipads etc in school				✓				✓
Use of school owned tablets/ laptops/ ipads in school but not for personal use	✓				✓			
Use of school owned tablets/ laptops/ ipads out of school but not for personal use	✓ with AUP						✓ Eg trips	
Only using school provided encrypted storage devices	✓				✓			
Use of school email for personal emails				✓				
Social use of chat rooms/facilities				✓				✓
Use of social network sites in school				✓				✓
Use of educational blogs	✓						✓	

Appendix 3

Acceptable Internet Use Policy – Pupils
This document is a guide to young people to be responsible and stay safe while using the Internet and other communication technologies. It clearly states what use of computer resources is acceptable and what is not. Irresponsible use may result in the loss of Internet or computer access, contact with parents or in the event of illegal activities contact with the police.

- I will only access the school network through my authorised username and password. I will not use the passwords of others.
- I will not use the school IT systems / devices for personal or recreational use, for accessing social media sites, on-line gaming, gambling, internet shopping, file sharing or video broadcasting.

- I will not try to upload, download or access any materials which are illegal, inappropriate or which may cause harm and distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place.
- I will not try to install programmes on any school computer or try to alter computer settings.
- I will only use my personal hand held devices (e.g. mobile phone/ipod) in school at times that are permitted. When using my own devices I understand that I have to follow the rules set out in this document.
- I will carefully write email and other on-line messages making sure the language I use is not strong, aggressive or inappropriate and shows respect for others. I am responsible for the emails I send and the contacts I make.
- I will not open emails unless I know and trust the person/organisation who has sent them.
- For my own safety and that of others, I will not disclose personal information about myself or others when on-line. I will not arrange to meet 'on-line friends'.
- I will not take, or distribute, images of anyone else without their permission.
- I will not take, or distribute, images of myself or anyone else semi-naked or naked.
- I will only use chat and social networking sites with permission and at the times that are allowed.
- I will report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- Where the material I research on the Internet is protected by copyright, I will not try to download copies, including music and video. I will only use the work of others found on the Internet in my own work with their permission.
- I will take care to check that information I find on the Internet is accurate and understand that some work found on the Internet can be untruthful or misleading.
- I will immediately report any damage or faults involving IT equipment, however this may have happened.

Pupil Signed ……………………………………………………………………………..
Date …………………………………….
Parent / Carer Signed …………………………………………………………………..
Date……………………………………

Appendix 4

Acceptable Internet Use Policy – Staff and other adults in school and Governors
Responsible Use Agreement
I understand that I must use the schools ICT systems in a responsible way to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that learners receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with students.
For my professional and personal safety:
- I understand that the school will monitor my use of ICT systems, email and other digital communications.
- I understand the rules set out in this agreement also apply to the use of the school ICT systems (e.g. laptops, email, Learning Platform etc.) out of the school.
- I will only use school ICT equipment / mobile phones for school purposes I will not use any personal devices for any school business
- I understand that the school ICT systems are intended for educational use and that I will not use systems for personal or recreational use.
- I will not disclose my username and password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material/incident I become aware of to the appropriate person

I will be professional in my communications and actions when using school ICT systems:
- I will not access, copy, remove or otherwise alter any other user's files without their express permission.

- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I am aware that emails can be part of Freedom of Information requests so all my correspondence will be professional, courtesy and respectful
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images.
- I will not use chat and social networking sites in the school in accordance with the school's policies.

I will only communicate with student and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will not befriend any present pupil or their family members on social media
- I will not 'discuss' any school issues on social media
- I will not use personal email addresses on the school ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not (unless I have permission) make large downloads or uploads that might take up Internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport and hold data about others that is protected by the Data Protection Act in an encrypted manner. I will not transfer any data to any personal devices.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the Internet in my professional capacity or for school sanctioned personal use:
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and, in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines.
Staff/Volunteer/ Governor
Name ………………………………………………………………………..
Signed ……………………………………………………………………….
Date ………………………………………………………………………….

Appendix 5

Appropriate / inappropriate Internet Activity

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable AND illegal
Child sexual abuse images					✓
Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✓
Adult material that potentially breaches the Obscene Publications Act in the UK					✓
Criminally racist material in the UK					✓
Pornography					✓
Promotion of any kind of discrimination				✓	
Any Hate Crime – motivated by hostility on the grounds of race, religion, sexual orientation, disability or transgender identity.					✓
Promotion of any kind of extremist activity					✓
Promotion of racial or religious hatred					✓
Accessing any extremist materials online (e.g Far Right Extremism)				✓	
Threatening behaviour, including promotion of physical violence or mental harm					✓
Any other information which may be offensive to colleagues or				✓	

breaches the integrity of the ethos of the school or brings the school into disrepute e.g discussing school issues on social media			✔		
Using school systems to run a private business				✔	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				✔	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✔	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				✔	
Creating or propagating computer viruses or other harmful files				✔	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				✔	
On-line gaming (educational)		✔			
On-line gaming (non-educational)				✔	
On-line gambling				✔	
On-line shopping / commerce			✔		
File sharing			✔		

Use of social networking sites			✓		
Downloading video broadcasting e.g. Youtube for educational purposes	✓				
Uploading to video broadcast e.g. Youtube			✓		

Appendix 6
Incidents involving pupils and actions to be taken

Incident involving pupils – either in school or out of school – it could be a concern raised by a friend/ parent	Teacher to use school behaviour policy to deal with	Refer to Senior member of staff	Record and monitor the pupils behaviour and refer to external agencies if required	Refer to technical support staff for action re security/filtering etc
A concern raised by a pupil/ teacher / friend/ parent (carer). A pupil need positive support – Signs of grooming Signs of peer on peer abuse / grooming / power domination Signs of radicalisation Signs of CSE Signs of cyberbullying		✓	✓	
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/ inappropriate activities).		✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓			✓
Unauthorised use of mobile phone/digital camera/ other handheld device.	✓			
Unauthorised use of social networking/ instant messaging/ personal email and online gaming	✓	✓		✓
Unauthorised downloading or uploading of files		✓		✓
Allowing others to access school network by sharing username and passwords		✓		✓
Attempting to access or accessing the school network, using another student's account		✓		✓
Attempting to access or accessing the school network, using the account of a member of staff		✓		✓
Corrupting or destroying the data of other users		✓		✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓		✓

Incident				
Continued infringements of the above, following previous warnings or sanctions		✓	✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓		✓
Using proxy sites or other means to subvert the school's filtering system		✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓		✓

Appendix 7
Incidents involving members of staff and actions to be taken

Incident involving staff / adults in school	Refer to the headteacher *see below	Refer to technical support staff for action re filtering / security	Potential Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /inappropriate activities).	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓		✓
Excessive or inappropriate personal use of the internet/social networking sites/ instant messaging/ personal email	✓	✓	✓
Unauthorised downloading or uploading of files	✓	✓	✓
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	✓	✓	✓
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓		✓
Deliberate actions to breach data protection or network security rules	✓	✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓
Using personal email/ social networking/ instant messaging/ text messaging to carrying out digital communications with students/ pupils	✓	✓	✓
Actions which could compromise the staff member's professional standing	✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓

Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓		✓

*In event of breaches of policy by the Headteacher, refer to the Chair of Governors.