Abbott Community Primary School

"Aiming high to achieve success!"

E-Safety Policy

Author: Kate Stokes
Date: August 2017
Ratified by Governors: September 2017
Review Date: August 2018

Contents:

- **AIMS**

.1 Abbott Community Primary's E-safety policy aims to create an environment where pupils, staff, parents, governors and the wider school community work together to inform each other of ways to use the Internet responsibly, safely and positively.

.2 Internet technology helps pupils learn creatively and effectively and encourages collaborative learning and the sharing of good practice amongst all school stakeholders. The e-safety policy encourages appropriate and safe conduct and behaviour when achieving this.

.3 Pupils, staff and all other users of school related technologies will work together to agree standards and expectations relating to usage in order to promote and ensure good behaviour.

.4 These agreements and their implementation will promote positive behaviour which can transfer directly into each pupil's adult life and prepare them for experiences and expectations in the workplace. The policy is not designed to be a blacklist of prohibited activities, but instead a list of areas to discuss, teach and inform, in order to develop positive behaviour and knowledge leading to a safer Internet usage and year on year improvement and measurable impact on e-safety. It is intended that the positive effects of the policy will be seen online and offline; in school and at home; and ultimately beyond school and into the workplace.

- **INTRODUCTION**

.1 Online safety is currently covered by the current Ofsted safeguarding guidelines.

.1.1 Ofsted have defined e-safety thus: *'In the context of an inspection, e-safety may be described as the school's ability to protect and educate pupils and staff in their use of technology and to have the appropriate mechanisms to intervene and support any incident where appropriate.'*

.1.2 E-safety will be inspected in relation to the following areas: "The behaviour and safety of pupils at the school," and "The quality of leadership in, and management of the school."

.1.3 Ofsted have identified three areas of e-safety risk in relation to pupils:

"Being exposed to illegal, inappropriate or harmful material."
"Being subjected to harmful online interaction with other users."
"Personal online behaviour that increases the likelihood of, or causes, harm."

.1.4 An outstanding school will demonstrate that: "All groups of pupils feel safe at school and at alternative provision placements at all times. They understand very clearly what constitutes unsafe situations and are highly aware of how to keep themselves and others safe, including in relation to e-safety."

.2 Ofsted will examine how the school:

- Audits the training needs of all staff and provides training to improve their knowledge of and expertise in the safe and appropriate use of new technologies
- Works closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and at school
- Uses pupils' and families' views more often to develop e-safety strategies
- Manages the transition from locked down systems to more managed systems to help pupils understand how to manage risk; to provide them with richer learning experiences; and to bridge the gap between systems at school and the more open systems outside school
- Provides an age-related, comprehensive curriculum for e-safety that enables pupils to become safe and responsible users of new technologies
- Works with partners and other providers to ensure that pupils who receive part of their education away from school are e-safe
- Systematically reviews and develops e-safety procedures, including training, to ensure that they have a positive impact on pupils' knowledge and understanding.
- Ensure pupils are aware of e-safety reporting procedures in school.

- Audits the training needs of all staff and provides training to improve their knowledge of and expertise in the safe and appropriate use of new technologies
- Works closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and at school
- Uses pupils' and families' views more often to develop e-safety strategies
- Manages the transition from locked down systems to more managed systems to help pupils understand how to manage risk; to provide them with richer learning experiences; and to bridge the gap between systems at school and the more open systems outside school
- Provides an age-related, comprehensive curriculum for e-safety that enables pupils to become safe and responsible users of new technologies
- Works with partners and other providers to ensure that pupils who receive part of their education away from school are e-safe
- Systematically reviews and develops e-safety procedures, including training, to ensure that they have a positive impact on pupils' knowledge and understanding.
- Ensure pupils are aware of e-safety reporting procedures in school.

.3 Key Features of good or outstanding practice:

- All staff understand e-safety issues. e-safety is a school priority. The school has, or is working towards an e-safety Mark. Training in e-safety is audited and provided to all staff. A number of members of staff have received accredited e-safety training. Pupils, parents, wider school community stakeholders and governors all contribute to build a fluid and constantly evolving e-safety policy.
- Clear and transparent procedures exist for monitoring, logging, reporting incidents, evaluating, improving and measuring the impact of e-safety. All staff, parents, pupils, contractors and governors know how to report an e-safety incident.

- The school uses recognised and accredited providers for Internet provision and filtering.
- The Online safety policy is closely integrated with relevant policies and procedures, including child protection, safeguarding, acceptable use, anti-bullying, anti radicalisation and behaviour.
- The acceptable use policy agreements have been developed with, signed by, and agreed to by all users of school IT systems – pupils, parents, staff, governors, visitors and external contractors.
- The school promotes a real world, responsible and positive outlook towards Digital Literacy and Citizenship and Online safety aimed at preparing pupils for expected standards of behaviour in adult life and the workplace.
- The school relies on government, DfE, National College for Teaching & Leadership and ICO guidance and documentation with regard to Data Protection, data storage and privacy compliance.

.4 E-safety Policy scope

.4.1 The school e-safety Policy and agreements apply to all pupils, staff, support staff, external contractors and members of the wider school community who use, have access to or maintain school and school related Internet, computer systems and mobile technologies internally and externally.

.4.2 The school will make reasonable use of relevant legislation and guidelines to affect positive behaviour regarding ICT and Internet usage both on and off the school site. This will include imposing rewards and sanctions for behaviour and sanctions for inappropriate behaviour – as defined as regulation of student behaviour under the Education and Inspections Act 2006. 'In Loco Parentis' provision under the Children Act 1989 also allows the school to report and act on instances of cyber bullying, abuse, harassment (including sexual harassment), malicious communication and grossly offensive material; including reporting to the police, social media websites, and hosting providers on behalf of pupils.

.5 The E-safety policy covers:

- School based ICT systems and equipment
- School based intranet and networking
- School related external Internet, including but not exclusively, e-learning platforms, blogs, social media websites
- External access to internal school networking, such as webmail, network access, file-serving (document folders) and printing.
- School ICT equipment off-site, for example staff laptops, digital cameras, mobile phones, tablets
- Pupil and staff personal ICT equipment when used in school and which makes use of school networking, file-serving or Internet facilities.
- Tablets, mobile phones, devices and laptops when used on the school site.

2.6 Reviewing and evaluating e-safety and ensuring good

The e-safety policy will be actively monitored and evaluated by an e-safety committee. This committee will comprise:

- E-safety Coordinator (Name)
- Head Teacher and School Leadership Team (Phillippa Wilson/Kate Stokes/Georgia Fishwick)
- Designated Safeguarding Lead (Phillippa Wilson)
- ICT technical support and Network Manager (One Education)
- Governor(s) (Name or refer to document)
- In the event of an e-safety incident, the following people will be informed within school and in external agencies and stakeholder organisations (Insert names, for examples: School e-safety Coordinator/Officer, DSO, Child Protection Officer, SLT, Trust CEO, nominated member, LA LADO, LA ICT director, CEOP, local police contact.)

- **THE E-SAFETY CALENDER**

.1 E-safety policy review and evaluation schedule:

.1.1 The e-safety policy and Acceptable Use Policy are reviewed at or prior to the start of each academic year.

.1.2 Additionally, the policy will be reviewed promptly upon:

- Serious and/or frequent breaches of the acceptable Internet use policy or other in the light of e-safety incidents.
- New guidance by government / LA / safeguarding authorities.
- Significant changes in technology as used by the school or pupils in the wider community.
- E-safety incidents in the community or local schools which might impact on the school community.
- Advice from the Police and/or Local Safeguarding Childrens Board

.1.3 The e-safety policy review will be documented in the school development plan and school self-evaluation and improvement profiling.

.1.4 The school will draw up an e-safety calendar detailing training, meetings, reviews, evaluations, teaching and learning provision, parental involvement, wider community involvement and governor involvement over an academic year. Regular use will be made of staff, parent and pupil e-safety audits, and pupil AfL questionnaires to inform e-safety learning, staff training requirements, gauge the impact and effectiveness of the e-safety provision and determine future e-safety targets.

.1.5 The e-safety calendar needs to include a schedule of events, which feed into the e-safety development or action plan.

.1.6 It is good practice to include parents, older pupils and peer-group pupils in e-safety presentations – to provide illustrative examples of e-safety issues.

.1.7 Evaluation, review, revision and training should be ongoing activities, linked into points in the yearly e-safety calendar.

.1.8 Liaison with feeder schools / secondary schools should be at fixed points in the e-safety calendar.

.1.9 Liaising with local schools regarding e-safety is good practice, for example creating an e-safety cluster group.

.1.10 LA – child protection, and safeguarding meetings should be referenced in the e-safety calendar.

.1.11 The Governing Body will receive a report on the progress, evaluation, impact and effectiveness of the e-safety policy [annually | biannually and suggest dates]. This report will include suitably redacted accounts and statistics of e-safety incidents and how these have been resolved, and counter measures implemented.

.1.12 The e-safety Coordinator will include in reports evaluations of the impact of the e-safety policy by evidencing – for example - e-safety incidents, contemporaneous written reports, statistics of filtering breaches, logs of Internet and network traffic activity, AfL teaching questionnaires and e-safety audits of staff, support staff, parents, governors and other stakeholders, ParentView and Ofsted questionnaire results.

- **ROLES AND RESPONSIBILITIES**

.1 School senior Leadership and E-safety

.1.1 SLT is responsible for determining, evaluating and reviewing e-safety policies to encompass teaching and learning, use of school IT equipment and facilities by pupils, staff and visitors, and agreed criteria for acceptable use by pupils, school staff and governors of Internet capable equipment for school related purposes or in situations which will impact on the reputation of the school, and/or on school premises.

.1.2 The e-safety policy is a result of a continuous cycle of evaluation and review based on new initiatives, and partnership discussion with stakeholders and outside organisations; technological and Internet developments, current government guidance and school related e-safety incidents. The policy development cycle develops good practice within the teaching curriculum and wider pastoral curriculum. Regular assessment of strengths and weaknesses help determine inset provision for staff and governors and guidance provided to parents, pupils and local partnerships.

.1.3 The e-safety provision is always designed to encourage positive behaviours and practical real world strategies for all members of the school and wider school community.

.1.4 Management is encouraged to be aspirational and innovative in developing strategies for e-safety provision which will deliver measurable success via a calendar of e-safety provision and clearly state e-safety targets with success criteria on the school development plan.

.2 School E-safety Coordinator

.2.1 The school has a designated e-safety officer [insert name] who reports to the SLT and Governors and coordinates e-safety provision across the school and wider school community.

.2.2 The school e-safety officer has a specific job description and person specification detailing the role, remit, qualifications and qualities required for the post. This specification is updated according to the school cycle for reviewing job descriptions.

.2.3 The school's e-safety coordinator chairs the school e-safety committee which includes representatives of the school SLT, teaching and support staff, governors, parents, pupils and the wider school community including relevant local stakeholders. Currently the e-safety committee comprises: [insert names]

.2.4 The school e-safety committee meets regularly at intervals defined in the school's e-safety calendar.

.2.5 The school e-safety coordinator is responsible for e-safety issues on a day to day basis and also liaises with LA/Trust contacts, filtering and website providers and school ICT support.

.2.6 The school e-safety coordinator maintains a log of submitted e-safety reports and incidents.

.2.7 The school e-safety coordinator audits and assesses inset requirements for staff, support staff and governor e-safety training, and ensures that all staff are aware of their responsibilities and the school's e-safety procedures. The coordinator is also the first port of call for staff requiring advice on e-safety matters.

.2.8 Although all staff are responsible for upholding the school e-safety policy and safer Internet practice, the e-safety Coordinator, the Child Protection Officer and ICT support [Change as required] are responsible for monitoring Internet usage by pupils and staff, and on school machines, such as laptops, used off-site.

.2.9 The e-safety Coordinator is responsible for promoting best practice in e-safety within the wider school community, including providing and being a source of information for parents and partner stakeholders.

.2.10 The school e-safety coordinator (along with IT support and the computing coordinator) should be involved in any risk assessment of new technologies, services or software to analyze any potential risks

.3 Governors

.3.1 At least one Governor is responsible for e-safety, and the school e-safety Officer/Coordinator will liaise directly with the Governor with regard to reports on e-safety effectiveness, incidents, monitoring, evaluation and developing and maintaining links with local stakeholders and the wider school community.

.3.2 To provide and evidence a link between the school; governors and parents, it is suggested that a parent-governor be appointed to this role. If other governors are included in this process, it is suggested that a further governor represents the role of the school in delivering e-safety education to other stakeholders and the wider school community. For example, this might be an LA or Trust appointed governor or a faith-based governor.

.3.3 An audit of Governor IT competence, relevant outside experience and qualifications is advisable to identify training needs and create a schedule and development plan. It is essential that Governors tasked with overseeing and monitoring e-safety have demonstrable experience, skills or qualifications to match the role.

.3.4 The e-safety Officer/coordinator will be responsible for auditing Governor e-safety training and inset requirements.

.4 ICT support and external contractors

.4.1 Internal ICT support staff and technicians are responsible for maintaining the school's networking, IT infrastructure and hardware. They need to be aware of current thinking and trends in IT security and ensure that the school system, particularly file-sharing and access to the Internet is secure. They need to further ensure that all reasonable steps have been taken to ensure that systems are not open to abuse or unauthorised external access, with particular regard to external logins and wireless networking.

.4.2 Support staff also need to maintain and enforce the school's password policy and monitor and maintain the Internet filtering.

.4.3 External contractors, such as VLE providers, website designers/hosts/maintenance contractors should be made fully aware of and agree to the school's e-safety Policy. Where contractors have access to sensitive school information and material covered by the Data Protection Act, for example on a VLE, school website or email provision, the contractor should also be DBS checked.

.4.4 Schools that outsource their IT e.g. connectivity, maintenance, cloud based services website and email provision, filtering and anti-virus need to ensure that they comply with D of E guidance and that a Service Level Agreement (SLA) is in place to provide school standard provision and support.

.5 Teaching and learning staff

.5.1 Teaching and teaching support staff need to ensure that they are aware of the current school e-safety policy, practices and associated procedures for reporting e-safety incidents.

.5.2 Teaching and teaching support staff will be provided with e-safety induction as part of the overall staff induction procedures.

.5.3 All staff need to ensure that they have read, understood and signed (thereby indicating an agreement) the Acceptable Use Policies relevant to Internet and computer use in school.

.5.4 All staff need to follow the school's social media policy, in regard to external off site use, personal use (mindful of not bringing the school into disrepute), possible contractual obligations, and conduct on Internet school messaging or communication platforms, for example email, VLE messages and forums and the school website.

.5.5 All teaching staff need to rigorously monitor pupil Internet and computer usage in line with the policy. This also includes the use of personal technology such as cameras, phones and other gadgets on the school site.

.5.6 Teaching staff should promote best practice regarding avoiding copyright infringement and plagiarism.

.5.7 Be aware of online propaganda and help pupils with critical evaluation of online materials.

.5.8 Internet usage and suggested websites should be pre-vetted and documented in lesson planning.

.6 Child Protection Officer

.6.1 The Child Protection Officer needs to be trained in specific e-safety issues. Accredited training with reference to child protection issues online is advised – for example a CEOP accredited course.

.6.2 The Child Protection Officer needs to be able to differentiate which e-safety incidents are required to be reported to CEOP, local Police, LADO, Local Safeguarding Children's Board, Trust CEO, social services and parents/guardians; and also determine whether the information from such an incident should be restricted to nominated members of the leadership team.

.6.3 Acting ‘in loco parentis’ and liaising with websites and social media platforms such as Twitter and Facebook to remove instances of illegal material or cyber bullying.

.6.4 Possible scenarios might include: Allegations against members of staff.

- Computer crime – for example hacking of school systems.
- Allegations or evidence of ‘grooming’.
- Allegations or evidence of cyber bullying in the form of threats of violence, harassment or a malicious communication.
- Producing and sharing of Youth Produced Sexual Imagery (YPSI)

1 Pupils:

Are required to use school Internet and computer systems in agreement with the terms specified in the school Acceptable Use Policies. Pupils are expected to sign the policy to indicate agreement, and/or have their parents/guardians sign on their behalf.

- Pupils need to be aware of how to report e-safety incidents in school, and how to use external reporting facilities, such as the Click CEOP button or Childline number.
- Pupils need to be aware that school Acceptable Use Policies cover all computer, Internet and mobile technology usage in school, including the use of personal items such as phones.
- Pupils need to be aware that their Internet use out of school on social networking sites such as Instagram is covered under the Acceptable Use Policy if it impacts on the school and/or its staff and pupils in terms of cyber bullying, reputation, YPSI or illegal activities.

Parents and Guardians:

- It is hoped that parents and guardians will support the school’s stance on promoting good Internet behaviour and responsible use of IT equipment and mobile technologies both at school and at home.
- The school expects parents and guardians to sign the school’s Acceptable Use Polices, indicating agreement regarding their child’s use and also their own use with regard to parental access to school systems such as extranets, websites, forums, social media, online reporting arrangement, questionnaires and the VLE.
- The school will provide opportunities to educate parents with regard to e-safety.

Other users:

- Other users such as school visitors, or wider school community stakeholders or external contractors should be expected to agree to a visitor’s AUP document or a tailored AUP document specific to their level of access and usage.
- External users with significant access to school systems including sensitive information or information held securely under the Data Protection Act should be DBS (formerly CRB) checked. This includes external contractors who might maintain the school domain name and web hosting – which would facilitate access to cloud file storage, website documents, and email.

1

Appendix A

Abbott Community Primary School

Social Media Usage Policy

Aims

To quickly share and celebrate children's achievements, successes and school updates on ***Facebook*** and ***Twitter***; to demonstrate safe and responsible use of social media.

Administration & Usage

The school social media accounts will:

- Be ran by a senior leader, from a school device.
- Be a Public account. **Senior leaders will monitor the followers and block any who appear to not be school focused.**
- Only tweet/post between the hours of 8am and 6pm between Monday and Friday. Tweets/posts outside of this time are for school events (e.g. football matches, residential trips, performances) or to share urgent school news (e.g. closers due to adverse weather).
- Only follow educationally linked accounts. No personal accounts, unless they are educationally linked, will be followed [e.g. a children's author.]
- Not reply to any 'replies' on Twitter. This is not the platform to discuss or debate school related issues.
- Only use children's first names when referencing children.
- Use tweets/posts to share positive messages about the school.
- Be used to share news and information during a school trip. The account will be ran by a senior teacher on a 3G connected phone for the period of the trip. Photos taken on the phone for the purpose of sharing on Twitter/Facebook will be deleted once they have been shared.
- Not include *Individually targeted content* e.g. "Well done Josh a better lesson today". Tweets/posts aimed at a year group or class along the lines of "don't forget the..." are acceptable.
- Avoid use of the @twittername of others.
- Adhere to Twitter & Facebook safety rules and guidelines.

Written by: K. Stokes

Review: September 2018

Appendix B

Abbott Community Primary School

Staff Safer Social Networking Practice Policy

This document applies to current social networking sites such as Facebook, Snapchat, Twitter, Instagram and all other current and emerging technologies.

a) **All adults** must adhere to, and apply the principles of this document in all aspects of their work. Failure to do so may lead to action being taken under the disciplinary procedure

b) In their own interests, adults within school settings need to be aware of the dangers of putting their personal information onto social networking sites, such as addresses, home or mobile phone numbers. This will avoid the potential for pupils or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties.

c) All adults, particularly those new to the school setting, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and/or the school if they were to be published outside of the site.

d) Adults should never make a ‘friend’ of a pupil at the school where they are working on their social networking page, and should be extremely cautious about becoming ‘friends’ with ex-students particularly where siblings or other relatives may continue to attend the school.

e) Staff should never use or access social networking pages of pupils

f) Confidentiality must be considered at all times. Social networking sites have the potential to discuss inappropriate information and employees need to ensure that they do not put any confidential information on their site about themselves, the school, the governing body, the Local Authority, their colleagues, pupils or members of the public.

g) Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, pupils or other individuals connected with the school, or another school, or the Local Authority could result in disciplinary action being taken against them.

h) Adults within the school setting must never post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring the school into disrepute or that could be interpreted as reflecting negatively on their professionalism.

i) Some social networking sites and other web-based sites have fields in the user profile for job title etc. As an employee of the school and particularly if you are a teacher or teaching assistant, you should not put any information onto the site that could identify either your profession or the school where you work. In some circumstances this could damage the reputation of the school and the profession.

j) This document does not replace or take priority over any advice contained in the school’s codes of conduct, or other policies issued around safeguarding or IT issues. It is intended to both supplement and complement any such documents.

Appendix C

Abbott Community Primary School

Staff, Governor and Visitors Acceptable User Policy & Agreement.

Our school promotes the positive use of technology in school and assists in developing pupils' knowledge and understanding of digital devices and the Internet. We ensure that our school IT network is robust and resilient and staff have a duty of care to safeguard pupils when using technology in school. Any misuse of technology by a pupil or member of staff must be reported to the Designated Safeguarding Person, so an investigation can take place.

IT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This is the Acceptable User Policy (AUP) for our school, which is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT.
The AUP covers the following legislation:

- Malicious Communications Act
- 1988 Data Protection Act 1998
- Computer Misuse Act 1990
- Communications Act 2003
- Sexual Offences Act 2003

All staff are expected to sign this policy and adhere at all times to its contents.

Using Technology in School

- I will only use school IT systems, external logins and email for school related purposes. Other use will be with the permission of SLT.
- I will monitor the use of all IT in school and report any inappropriate use by pupils or staff to the Designated Safeguarding Lead (DSL).
- I will not search for, view, download, upload or transmit any material which could be considered illegal, offensive, extremist defamatory or copyright infringing.

Security, Passwords & Copyright

- I will not divulge any school related passwords and I will comply with school IT security procedures.
- I will use school email systems for school related communications. I will not use personal accounts for school business.
- I will ensure that personal data is stored securely and in line with the Data Protection Act. I will follow school policy with regard to external logins, encrypted data and not storing school material on personal IT equipment unless stated otherwise.
- I will not install software onto the network or mobile devices unless supervised by

the Network Manager or IT support staff.

Social Media

- I must maintain my professionalism at all times when using personal social media and not bring the school or my profession into disrepute by posting unsuitable comments or media when using these sites.
- I must not use social media tools to communicate with current or former pupils under the age of 18.
- I will only use authorised school social media accounts to post information to pupils or parents.

Mobile Technologies

- I will ensure that my mobile phone and any other personally-owned device is switched off or switched to 'silent' mode when I have directed time with pupils. I will only make or receive calls in specific places e.g. staffroom, workroom
- I will not contact any parents or pupils on my personally-owned device.

Online Professionalism

- I am aware that all network and Internet activity is logged and monitored and that the logs are available to SLT in the event of allegations of misconduct.
- I will not write or upload any defamatory, objectionable, copyright infringing or private material, including images and videos, of pupils, parents or staff on social media or websites in any way which might bring the school into disrepute
- I will make sure that my Internet presence does not bring the teaching profession into disrepute and that I behave online in line with the Teacher Standards (2012) and other guidelines from the DfE.
- I will champion the school's e-safety policy and be a role model for positive and responsible behaviour on the school network and the Internet.
- I will not give my home address, phone number, mobile number, personal social networking details or email address to pupils. All communication with parents should be done by authorized school contact channels.
- Photographs of staff, pupils and any other members of the school community will not be used outside of the internal school IT network unless written permission has been granted by the subject of the photograph or their parent/guardian. I will ask the permission of the Head Teacher prior to taking any photographs.

Signed: ______________________________

Name: ______________________________

Date: ______________

Appendix D

Abbott Community Primary School

Pupils Acceptable User Policy & Agreement

Our school promotes the use of technology in school as all pupils will need the skills and knowledge in whatever field of work they enter when they become an adult. We ensure that our school IT network is robust and resilient and we do our upmost to ensure the safety of children when using it. It is important that pupils abide by the school rules when using technology in school and inform a member of staff immediately, if they become aware of any misuse.

This is the Acceptable User Policy (AUP) for our school. It highlights the do's/don'ts of using all technology in school and shows how we want pupils to behave when using IT. Any misuse will result in pupils being temporarily banned from using the school network and may result in exclusion at the Head teacher's discretion.

Please read carefully and sign at the bottom to show you agree to these terms. If you do not sign and return this form you will not be able to use the IT systems in school.

For Pupils:

Using Technology in School

- I will only use the school Internet and network for my school work or when a teacher has given permission.
- I will not try and bypass the schools Internet settings.
- I will not look at, change or delete other people's work or files.
- I will be careful with keyboards, mice, headphones and all other equipment, and when turning a computer on or off.
- I will be sensible when using mobile technologies and follow the rules about moving about the school when using them.
- I will follow the rules about bringing my own personal device into school e.g. smartphone and/or smartwatch.

Security & Copyright

- I won't upload or download any pictures, writing or movies which might upset people or make other people think the school is a bad place.
- I will use non-copyrighted images and music from the Internet when creating documents, presentations or other media.
- I won't try to install software onto the school network because it might have a virus on and cause a lot of damage. Instead I will ask a teacher for advice.

Online Behaviour & Safety

- I won't give out my personal details, such as my name, address, school or phone number on the Internet or when registering for a software app.
- I won't meet people I've met on the Internet unless I have told my parents and they come with me.
- I will make sure all my contact with other people at school is responsible. I will not cyber bully

pupils, teachers or other members of staff.

- I won't look for or look at unpleasant or inappropriate web sites or software apps. I will check with a teacher if I think it might be unsuitable.
- I know that everything I do on the computers at school is recorded and that the school can talk to my parents if a teacher is worried about my online safety.
- I will try to follow these rules all the time because I know they are designed to keep me safe.

For Parents:

- I agree to support and uphold the principles of this policy in relation to my child and their use of technology and the Internet, at home and at school.
- I agree to uphold the principles of this policy in relation to my own use of the Internet, when that use is related to the school, employees of the school and other students at the school.
- Images of pupils will only be taken, stored and used for school purposes in line with school policy. Images will only be used on the Internet, in the press, or in media, with permission.

Pupil: ____

Parent/Guardian Signed: ____

Date: ____________________