E-Safety POLICY

September 2019

Date approved by the 'D and P' Committee …….
Signed by Chair of Governors ...……..
Signed by Head Teacher …….
Date of next review ……

1. Introduction to e-safety

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.
Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently, the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook, Instagram and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting including YouTube
- Music Downloading

The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

Whilst exciting and beneficial, both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements, usually 13 years.

At Priory Junior School we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

2. Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are correctly embedded and monitored. The named e-safety co-ordinator in this school is *the headteacher* who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the e-safety co-ordinator to keep abreast of current issues and guidance through organisations such as Notts LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet. Senior Management and governors are updated by the Head/ e-safety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and SMSC.

3. E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote e-safety.

The school provides opportunities within a range of curriculum areas to teach about e-safety. Some of the resources that the children will be using are listed below.

- Be Internet Legends (Sharp, Alert, Secure, Brave, Kind)
- ThinkuKnow
- NSPCC Learning – Share Aware
- Internet Matters

Other websites that are recommended to be used across the school are:

- http://www.childnet.com
- http://www.childnet.com/resources/the-adventures-of-kara-winston-and-the-smart-crew
- http://www.kidsmart.org.uk/

- https://www.thinkuknow.co.uk/

Educating pupils about the online risks that they may encounter outside school is done as part of the e-safety curriculum and informally when opportunities arise.

Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button.

The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Pupils will be made of aware of this and the relevant legislation when using the internet, such as data protection and intellectual property which may limit what they want to do, but also serves to protect them.

Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modelling and appropriate activities

Pupils will also be taught to be critically aware of the materials they read and be shown how to validate information before accepting its accuracy.

4. **E-safety Skills Development for Staff**

- Our staff receive regular information and training on e-safety and how they can promote the 'Stay Safe' online messages in the form of a variety of training including family of schools training and CPD from the computing or e-safety lead.
- Details of the ongoing staff training programme can be found in the School Development Plan.
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety and know to inform the e-safety coordinator and Head teacher in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas.

5. Managing the School e-safety Messages

We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used. The e-safety policy will be introduced to the pupils at the start of each school year and e-safety posters will be prominently displayed. The key e-safety advice will be promoted widely through the school community through displays, newsletters, the School Website, our Learning Platform, class activities, parent workshops, themed weeks, assemblies and when any issues arise.
The e-safety message is weaved into a range of curriculum areas and staff actively seek opportunities to re-iterate this message. The schools PRIDE values are also used to promote a message of being safe online and encourage pupils to take responsibility for their online safety.

6. Managing Internet Access

Information system security

School ICT systems capacity and security will be reviewed regularly.
Virus protection will be updated regularly.
Security strategies will be discussed with EMBC and ICT services.

Published content and the school web site

The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information will **not** be published.
The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

Photographs 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 or Learning Platform (public area) or Blog, particularly in association with photographs.
Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website or Learning Platform (public area).
Pupil's work can only be published with the permission of the pupil and parents.
See GDPR documentation for further details.

Social networking and personal publishing

The school will block / filter access to social networking sites.
Newsgroups will be blocked unless a specific use is approved.
Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils and can easily access further information through the school (and our work with the NSPCC) on the age restrictions relating to specific sites.
Many of the issues that face children currently have involved the use of:

- **Skype** - a video and messaging app. You are required to be at least 13 years old before you can create an account
- **Snapchat** - a photo and video sharing app allowing images and texts to be sent and automatically deleted after a set amount of time. You are required to be at least 13 years old before you can create an account
- **Instagram** - an online mobile photo sharing, video sharing and social networking service which enables its users to take pictures and videos and share them on a variety of social networking platforms. You are required to be at least 13 years old before you can create an account
- **Facebook** - a social networking site. You are required to be at least 13 years old before you can create an account
- **WhatsApp** – An instant messaging app for smartphones. The user agreement requires users to be age 16 or older. Children are often creating 'groups' to which others are joining. This means that all information is shared with anyone who is in the group so privacy is lost and in some cases strangers have been added to the group
- **Fortnight** - a group game where children can be muted and excluded from groups. The recommended age for this game is 13 years

Managing filtering

The school will work with the LA, DCSF and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
If pupils or staff discover an unsuitable site, it must be reported to the Class Teacher, e-Safety Coordinator or Headteacher.
Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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.
The use of portable media, such as memory sticks, SD cards, external hard drives and CD ROMS, will be monitored closely as potential sources of computer virus and inappropriate material.
Pupils' with permission to bring mobile phones to school will give them to teaching staff at morning registration, these are locked away, then returned to pupils at the end of the school day.
Staff will use a school phone where contact with pupils is required.

Staff should not use personal mobile phones during designated teaching sessions, unless in an emergency. Staff across school ensure that their personal mobile devices are locked away during contact hours with pupils.

Protecting personal data

All personal data is protected and kept securely by the school. Please see our GDPR policy/documentation for details on this.

7. Policy Decisions

Authorising Internet access

Pupil instruction in responsible and safe use should precede any Internet access and all pupils must sign up to the Pupil e-Safety rules which will form part of the home school agreement.
Signing of these rules will show that the child agrees to abide by the school's e-Safety Rules.
These e-Safety Rules will also be displayed clearly in all networked rooms.
All parents will be asked to sign the Parent e-Safety Agreement giving consent for their child to use the Internet in school by following the school's e-Safety Rules and within the constraints detailed in the school's e-Safety Policy.
All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor EMBC can accept liability for the material accessed, or any consequences of Internet access.
The SLT and the ICT co-ordinator will audit ICT provision annually to establish if the e-Safety Policy is adequate and that its implementation is effective.

Handling E-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff.
Any complaint about staff misuse must be referred to the Headteacher.
Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
Pupils and parents will be informed of the complaints procedure.

Community use of the Internet

External organisations using the school's ICT facilities must adhere to the e-Safety Policy.

8. Communications Policy

Introducing the e-Safety Policy to pupils

E-safety rules will be discussed with the pupils at the start of each year.
Pupils will be informed that network and Internet use will be monitored.
E-safety is then embedded into the computing and wider curriculum to ensure pupils receive a consistent and regular message regarding their online safety.

Staff and the e-Safety Policy

All staff will be given the School E-Safety Policy and its importance explained.
Any information downloaded must be respectful of copyright, property rights and privacy.
Staff should be aware that Internet traffic can be monitored and traced to the individual user.
Discretion and professional conduct is essential.
A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software.

Enlisting parents' support

Parents' attention will be drawn to the School E-Safety Policy in newsletters, the School Prospectus, on the Learning Platform and the School Website.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute

- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with GDPR with regards the use of such images
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers

9. **Monitoring and review**

This policy is implemented on a day-to-day basis by all school staff and is monitored by the E-Safety Co-ordinator. The headteacher and deputy headteacher will monitor the implementation of this policy, and will submit periodic evaluation reports on its effectiveness to the governing body. This policy will be reviewed in three years, or earlier if necessary.

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-Safety issues	Relevant websites
Using search engines to access information from a range of websites.	Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Google Yahooligans CBBC Search
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should use only approved e-mail/chat accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. Super Clubs.	email a children's author email Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	School website Making the News Infomapper Focus on Film
Publishing images including photographs	Parental consent for publication of	Making the News Seesaw

of pupils.	photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	School website and any other site not named here.

Appendix 2: E-safety rules for children (displayed in networked areas e.g. ICT suite)

- Keep passwords safe, they should not be shared.
- When online, never give out any of your details (name, address, email address etc) without permission from a parent/ carer or teacher.
- Inappropriate use of the internet will result in a verbal warning
- Misuse may result in you not being allowed to use the internet for a set time
- Report to your teacher or parent any inappropriate use of technology (e.g. Internet, mobile phones etc)

10 Rules for Online Safety

1.  Keep personal information such as your date of birth, telephone number, address, name/location of your school, parents' work address/telephone number private. 

2. Report any information that makes you feel uncomfortable to your parents or my teacher. 

3.  Never agree to get together with someone you "meet" online unless your parents agree and come with you to meet them in a public place.

4. Never send a person your picture or anything else without first checking with your parents.

5.  Never respond to any mean or unkind messages. Tell parents/teacher if any messages make you feel uncomfortable.

6. Set up rules for going online with your parents about the time of day, the length of time and appropriate areas for you to visit. Stick to them!

7.  Never give out internet passwords to anyone (even your best friends) other than parents.

8. Check with an adult before downloading or installing software or doing anything that could possibly hurt the computer or jeopardize your family's privacy.

9.  Be a good online citizen and do not do anything that hurts other people or is against the law.

10. Help your parents understand how to have fun and learn things online. Teach them about the tech you are using!

SMARTthinking

S	Safe   **STOP and THINK** **Will the information you share keep you safe?**
M	 Meeting **STOP and THINK** **Are your online friends who they say they are?**
A	Accepting  **STOP and THINK** **How do you know files and pictures are safe?**
R	Reliable  **STOP and THINK** **How do you know that people or pages aren't lying?**
T	Tell  **STOP and THINK** **Who can you tell if you feel uncomfortable about something online?**

Appendix 3: Nottinghamshire County Council's Guidance on the Acceptable Use of ICT in Schools.

Nottinghamshire County Council

Guidance on the Acceptable Use of ICT in Schools

30 November 2019

E-Safety Policy by C Graham

1. INTRODUCTION

1.1 This guidance applies to the safe use of ICT equipment and services provided by a school. School Governors and head teachers are asked to adopt this guidance and implement it throughout their school.

1.2 Any changes to this guidance will be communicated to schools through the Council's Children and Young People's Services.

1.3 Anyone discovering a breach of this guidance, or who is in receipt of electronic communication that appears to contravene the guidance described below, should raise the issue with the head teacher in the first instance.

2. PURPOSE AND SCOPE

2.1 The purpose of this guidance is to:

- Provide direction and guidance in the use of ICT;
- Encourage consistent and professional practice in the use of ICT;
- Protect School and users from inappropriate usage, security risks and legal liability;
- Ensure that all users are clear about their responsibilities in using ICT;
- Advise users on the monitoring arrangements for the usage of ICT.

2.2 This document applies to:-

- All permanent, temporary and casual staff working at a school;
- Pupils;
- Consultants, contractors, agency staff, governors, parents and others working at the school, including those affiliated with third parties who may be given access to ICT services.

(Note: Throughout this guidance, the word "user" is used to cover all of the above.)

3. TERMS USED WITHIN THIS DOCUMENT

- Appropriate: activities listed are acceptable in terms of ICT use.

- Inappropriate: activities listed as inappropriate may potentially lead to misconduct and disciplinary proceedings. In some cases this could lead to dismissal and legal action.

.

4. PASSWORDS

4.1 The school is responsible for establishing and enforcing a password policy for its use of ICT. The head teacher is responsible for establishing and enforcing a password policy on their systems based on the level of security required. Passwords must be assigned to individual users of ICT systems to maintain security and the data that they contain.

Appropriate:

- Users only using their own account to carry out day to day work;
- Users not disclosing their password to allow others to access their account. Users should be aware passwords are for the benefit of the school and are the proprietary and confidential information of the school;
- Users selecting a password that is easy to remember but not for others to guess;
- Users not selecting obvious passwords, such as the name of a close relative, friend or pet;
- Compliance with the password policy for each computer system.

Inappropriate:

- Requesting passwords personally assigned to other users;
- Using a session via another users password;
- Sharing passwords with other users. All users must take reasonable precautions to protect their passwords;
- If a user thinks that their username or password has been used without their permission, they must change the password and inform the head teacher as soon as practically possible. The head teacher will ensure that new users are issued with appropriate usernames and passwords. When a user leaves their job, whether leaving the school or not, the head teacher will ensure that all usernames and passwords for that user are suspended as appropriate.

5. USE OF E-MAIL AND INTERNET (including Social Media)

5.1 It is the responsibility of a school to ensure that all users use e-mail and Internet service in an acceptable manner and in accordance with the schools acceptable use policy and any e-mail and Internet agreements established by the school. Schools should use Nottinghamshire County Council's email and Internet code of practice for schools to establish their own policies on the acceptable use of email and internet.

5.2 The Internet provides users with access to worldwide information services, bringing new opportunities for communication. With the increasing popularity of social media tools such as Facebook and Twitter thought

should be given when using these tools for publishing information about a school.

5.3 Social media tools are excellent tools for teaching and learning and can provide exciting, new opportunities for schools to engage, communicate and collaborate with users and the wider community.

5.4 Whilst social media tools can provide tremendous benefits to schools they also have serious security risks in their use. Risks such as people posting unsafe or inappropriate information about themselves and their personal lives online as well as providing opportunities for offenders to groom and exploit children. In order to mitigate these security risks and still enjoy the benefits of social media schools should establish and enforce good social media usage policies which should include the following points:

- Supervision in the classroom with social media technology must be appropriate to the children's needs and abilities;
- It is good practice for staff to evaluate websites before classroom use. Staff should be aware that websites, search results etc. may be safe and appropriate one day but unsafe a day later. All members of the school community should be aware that filtering software is not always effective and cannot always be relied on alone to safeguard children;
- Children with Special Educational Needs should be appropriately supported according to their specific needs and their personal understanding of the e-Safety risks;
- All pupils and staff should be aware of the school procedure regarding what to do if inappropriate content or messages are found, sent or received online;
- All pupils and staff should understand how to critically evaluate online content;
- Internet filtering must be in place according to the school's requirements. This should be designed with both a technical and curriculum focus and should be agreed by the schools Leadership Team and Governors;
- ICT tools provided by the school should always be used (e.g. work provided digital cameras, memory cards, laptops etc.) rather than personally owned equipment.

6. USE OF PCs, LAPTOPS & SERVERS

Appropriate:

- Storing school data;
- Loading text, images, video or audio streams in connection with day to day work activities;
- Storing limited amounts of personal data (where agreed by the head teacher).

Inappropriate:

- Loading unauthorised or untested software;
- Allowing unauthorised users to access laptops used away from school;
- Failure to keep laptops used away from school secure;
- Storing confidential or personal data or information on removable media without adequate protection or encryption;
- Deliberate, reckless or negligent introduction of viruses;
- Storing personal material protected by copyright which has not been purchased;
- Loading files containing pornographic offensive or obscene material.

7. THE LEGAL FRAMEWORK

7.1 ICT use in a school setting should be legally regulated, this includes the content of e-mail, or sites downloaded from the Internet; privacy issues, monitoring of communications and surveillance at work and employment relations. Further legal advice should be sought, if appropriate, from Council's Children and Young people's Services HR or Legal Services.

7.2 If the school monitors e-mails or scans for profanity/inappropriate content then users should be warned of this through policies.