Contents

1. Policy on E-Safety and E-Learning

Aims

At Priory CE Primary School, we acknowledge the importance of technology the education and wider learning of our children. We consider it a priority to ensure that children are taught to us such technology safely and to encourage them to be responsible members of the online community.

'Today's children and young people are growing up in a digital world. As they grow older, it is crucial that they learn to balance the benefits offered by technology with a critical awareness of their own and other's online behaviour, and develop effective strategies for staying safe and making a positive contribution online.' (Education For a Connected World – UKCCIS 2018)

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils, staff, parents and governors about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students, encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Stoke-on-Trent Education WAN including the effective management of Web filtering.
- National Education Network standards and specifications.
- Complying with the General Data Protection Regulation (GDPR).

Teaching and learning

Why are new technologies and Internet use important?

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

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and will be 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 effective knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

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

- E-Safety co-ordinator will research new trends in apps, websites and content and liaise with the E-Safety Council to ensure they are covered in the teaching of E-Safety in classes.

Pupils will be taught how to stay e-safe

- Curriculum planning (see section 8) will include age appropriate opportunities to discuss, role play and learn about the benefits and risks offered by new technologies, such as video and photo-sharing apps, mobile phones and social networking sites.
- E-safety delivery will be mapped across the curriculum to ensure full coverage. This will be driven by the Education for a Connected World (2018) document and the structured around the 8 strands of this: Self Image and Identity, Online Relationships; Online Reputation; Online Bullying; Managing Online Information; Health Well-being and lifestyle; Privacy and Security; Copyright and Ownership.
- 'Children will be taught to identify possible online risks and make informed decisions about how to act.' (Teaching Online Safety in School, DfE 2019). This will develop a proactive approach and encourage children to report any risks they have encountered to a responsible adult.
- Annual E-Safety surveys will highlight trends in usage of technologies by children and pick up any dangerous behaviour.
- Safe password habits and behaviours will be taught to all children in everyday usage, relevant to use in and out of school
- Pupils are to be taught that 'the same standard of behaviour and honesty apply on and offline, including the importance of respect for others.' (Teaching Online Safety in School, DfE 2019)

Managing Internet Access

Monitoring Access

- Monitoring software is used to ensure children are safe from threats to their safety, including terrorist and extremist material, when accessing the internet in school.
- Regular reports are generated and scrutinised by the Computing coordinator. Any concerns are investigated using screen grabs from the flagged device. Records of words investigated are kept and any serious incidents are reported to the Headteacher.
- In the event that a child is found to have inputted inappropriate content or visited potentially unsafe sites, the child/children discuss this with the Computing co-ordinator. The Headteacher and parents, if necessary, are informed. Any issues are then logged on CPOMS system (from July 16). Sanctions are run in-line with the school behaviour policy for serious issues.
- Word banks containing reference to the following are flagged and reported:
  Racism and violence
  Suicide and health
  Drugs and addiction
  Acronyms and general slang
  Predators and strangers
  Swear words and profanities
  Sex words and slang
  Pornographic content
  Sexual health and biology
- In investigating the concerns, content will be flagged as 'False Positive' where a context is given to explain the presence of inappropriate content where the child is not responsible for this.
- Updates to the monitoring software are completed, where possible, to ensure the most up to date versions are used. Working with the school ICT Technician and the forensic software provider, the Computing co-ordinator will work to establish the most complete coverage of monitoring possible, including with emerging technologies.
- If staff or pupils discover an unsuitable site, the URL must be reported to the school filtering manager (nominated contact), the Computing Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Inappropriate content searched or inputted by children will be reported in termly E-Safety section of the report to Governors.

Information system security

- Virus protection will be updated regularly on all networked computers.
- School ICT systems capacity and security will be reviewed regularly.
- Filtering requests will be monitored and logged weekly with any teachers being made aware of inappropriate searches involving their class/Key Stage.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Emails containing confidential information will be encrypted through Office 365 software

Public Web 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.

- E-mail addresses will be published carefully, to avoid spam harvesting.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Web Publishing pupils' images and work

- Images published to the web will only include pupils for whom parental consent has been given.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written consent from parents or carers is obtained before images of pupils are electronically published to the web.

Social networking, Video Messaging and personal publishing

- The City Council/school will block/filter access to social networking sites, except those specifically purposed to support educationally approved practice.
- Staff and pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Staff and pupils will be advised not to publish specific and detailed private thoughts on social networking sites or blogs (See Section 3).
- Staff and pupils will be advised against video messaging and use of video messaging in school will be banned unless required as part of a specific lesson (e.g.- Speaking to link schools abroad).
- Apps including video and image sharing (eg. Snapchat, TikTok, Instagram) will be included in E-Safety lessons and children will told of the dangers of these.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out and protocols established before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time, unless specifically allowed to support learning as identified by the teacher. The sending of abusive or inappropriate text messages is forbidden. (See Section 4)
- Smart watches with the capability of either recording images, communicating off site or accessing the World Wide Web are treated as mobile phones, and as such should be handed to the teacher at the start of the day.

Protecting personal data

- Personal data will be recorded, processed, stored, transferred, retained and disposed of in accordance with the General Data Protection Regulation (GDPR).

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Staff Acceptable Use Policy' before using any school ICT resource. (see Section 5)
- At Key Stage 1 access to the Internet will be by adult demonstration or by directly supervised access to specific, approved on-line materials.
- All pupils will be asked to sign the 'Pupil Acceptable Use Policy' upon logging in to networked computers (see Section 6).
- Parents will be asked to sign and return a 'Parent Acceptable Use Policy' (see Section 7).
- Sanctions for inappropriate use will be drawn up and shared with staff and pupils.

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 Stoke-on-Trent City Council can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- 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.

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.
- E-Safety issues which raise a safeguarding alarm are recorded through the CPOMS system. Details of the incident are included, along with any follow up actions that have taken place. These incidents are to be logged under the following categories: Cyberbullying, Inappropriate Materials, Sexual Behaviour, Stranger Contact, Unsafe Behaviour.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions within the school discipline policy will include:
    - interview/counselling by the class teacher;
    - informing parents or carers;
    - removal or restriction of Internet or computer access for a period.

Cyberbullying – Understanding and addressing the issues

While cyberbullying is likely to be low level in primary schools the age of pupils making proficient use of technology is ever decreasing. Therefore, the opportunities for pupils to bully or be bullied via technology, such as during online gaming, e-mail, texts or social networking sites, are becoming more frequent.

As such, teaching pupils about appropriate behaviours when using technology provides a vital grounding for future use. Whilst not wanting to provoke unrecognised opportunities in pupils, consideration must be given to suitable teaching and procedures to address any issues of cyberbullying.

As felt appropriate for the age and use of technology by the pupils:

- The school's anti-bullying policy and/or school behaviour policy will address cyberbullying. Cyberbullying will also be addressed in Computing, PHSE and other relevant lessons and is brought to life through activities. As with other whole-school policies, all staff and young people will be included and empowered to take part in the process.
- Pupils, parents, staff and governors will all be made aware of the consequences of cyberbullying. Young people and their parents will be made aware of pupils' rights and responsibilities in their use of new technologies, and what the sanctions are for misuse.
- In cases where incidents occur outside of the school environment, the school is committed to investigate and communicate with parents involved. School sanctions can also be used as a result of this behaviour.
- In the event of staff being contacted or referred to in negative or insulting posts online, parents will be required to discuss this with the Headteacher and pupils involved.
- Parents will be provided with an opportunity to find out more about cyberbullying through: sessions for parents, guidance, social media communications, internet links etc.

Cyberbullying - How will risks be assessed?

The school will take all reasonable precautions to monitor and deal with cyberbullying, whilst pupils are in its care. However, due to the global and connected nature of new technologies, it is not possible to guarantee that inappropriate use via a school computer will not occur. Neither the school, nor Stoke-on-Trent City Council, can accept liability for inappropriate use, or any consequences resulting outside of school.

The school will proactively engage with all pupils in preventing cyberbullying by:

- understanding and talking about cyberbullying, e.g. inappropriate use of e-mail, text messages;
- keeping existing policies and practices up-to-date with new technologies;
- ensuring easy and comfortable procedures for reporting;
- promoting the positive use of technology;
- evaluating the impact of prevention activities.
- records of any incidents of cyberbullying will be kept and will be used to help to monitor the effectiveness of the school's prevention activities. (Appendix 5)
- 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.

How will cyberbullying reports/issues be handled?

- Complaints of cyberbullying will be dealt with by a senior member of staff.
- Governing Body to be advised of the fact that there are current issues.
- Any complaint about staff misuse must be referred to the headteacher.
- Evidence of offending messages, pictures or online conversations will be reported via the CPOMS system, in order to demonstrate to others what is happening. It can be used by the police to investigate the cyberbullying, where necessary.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions within the school discipline policy include:
    - interview/counselling by the class teacher;
    - informing parents or carers;
    - removal of Internet/computer access for a period or banning of mobile phone in school.

Communications Policy

Introducing the e-safety policy to pupils

- Priory E-safety rules will be posted in all networked rooms and discussed with pupils at the start of each year and as the need arises. (Section 10)
- Pupils will be informed that network and Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- An E-Safety curriculum will be included in Computing programmes covering both school and home use.
- An E-safety desktop background and posters in school will reinforce E-Safety methods

Staff and the E-Safety policy

- All staff will be given the School E-Safety Policy within the Staff Handbook and its application and importance explained.
- All staff will be informed that all computer and Internet use will be monitored. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use and on the school E-Safety Policy will be provided as required.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff will be made aware of expectations regarding social media, through the Staff Handbook and code of conduct.

Enlisting parents' support

- Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure, on the school website and through parents' sessions.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Regular updates of any ongoing concerns will be, where appropriate, communicated to parents via letter, Class Dojo or the school Facebook page.
- Parents are asked not to share images containing images of other children on social media.

2. Policy on the Use of Photography

Introduction

At Priory we welcome positive publicity. Photographs and video clips add colour, life and interest to school activities and initiatives and help the school community to identify and celebrate the school's achievements. We recognise that images must be used in a responsible way, respect young people's and adults' rights of privacy and are aware of child protection issues. However, we need to balance the risk against promotion. Risks can be minimised by following the guidelines detailed in this policy.

Data Protection

Photos and video images of pupils are classed as personal data under the terms of the General Data Protection Regulation. For this reason, we require the consent of their legal guardians before we can display these images in the media, in publications, on websites or in public places. (See Data Protection Policy)

Child Protection Issues

Risk occurs when individual pupils can be identified by their names alongside photographs. Therefore, we will give the Christian name of the children in photographs that are displayed within the school building. We will not provide names for any other purpose unless special parental consent has been received. Only images of children in suitable dress will be taken. Should the school learn about any inappropriateness of image use involving our pupils, we will immediately act and report it as we would for any other child protection issue.

Images taken by school staff

- Staff should not use recording equipment on their mobile phones, for example: to take recordings of children. If, however, a significant learning opportunity, or a considerable benefit to the wider curriculum, would be otherwise missed, staff may use them with discretion. Recordings must be downloaded to secure networks and then removed from the personal device at the soonest opportunity.
- Legitimate recordings and photographs should be captured using school devices: eg. cameras and iPads.
- Staff should report any usage of mobile devices that causes them concern to the DPO (Mr Facey).

Images taken by adults other than school staff

The school encourages parents/careers to take videos and photographs of school events. However, if any image is taken by either a parent/carer or third party with a view of publication in the press then the permission of the Headteacher must be obtained and special parental consent given. The school regularly reminds parents that images of children (other than their own) should not be posted online on social media etc.

When a commercial photographer/film maker (e.g. Academy) is used we will:

- Provide a clear brief
- Issue identification
- Inform parents and children
- Obtain consent
- Not allow unsupervised access to children

Images taken by children

The school encourages children to take photographs and videos of each other as a way of recording events. This may take place in school, on school trips or on residential visits. The use of cameras within school, on trips or visits is part of the pleasure and the learning in the experience. There is no reason why pupils should not be allowed to take photographs so long as anyone photographing respects the privacy of the person being photographed. This is seen as part of the school's code of behaviour. Infringement of this respect of privacy is akin to bullying and will be dealt with in the same way as any other branch of school discipline.

3. Policy on Social Media

Objectives

This policy sets out Priory CE Primary School's policy on social networking. Social networking activities conducted online outside work, such as blogging, involvement in social networking sites such as Facebook or Twitter and posting material, images or comments on sites such as YouTube can have a negative effect on an organisation's reputation or image. This policy has been written to set out the key principles and code of conduct that we expect of all members of staff with respect to their responsibilities in connection with the use of social networking sites.

Key Principles

- Everyone at Priory has a responsibility to ensure that they protect the reputation of the school, and to treat colleagues and members of the school with professionalism and respect.
- It is important to protect everyone at Priory from allegations and misinterpretations which can arise from the use of social networking sites.
- Safeguarding children is a key responsibility of all members of staff and it is essential that everyone considers this and acts responsibly if they are using social networking sites out of school. Anyone working in the school either as a paid employee or volunteer must not communicate with children via social networking.
- This policy relates to social networking outside work.

Code of Conduct: Social Networking

Under no circumstances should staff make negative reference to any staff member, pupil, parent or school activity/event.
The following are also **not considered acceptable**:

- The use of the school's name, logo, or any other published material without prior permission from the Headteacher. This applies to any published material including the internet or written documentation.
- The posting of any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments.
- The disclosure of personal data, confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.
- The posting of any images of employees, children, governors or anyone directly connected with the school whilst engaged in school activities.

In addition to the above everyone must ensure that they:

- Never 'friend' a pupil at the school where they are working onto their social networking site.
- Do not make any derogatory, defamatory, rude, threatening or inappropriate comments about the school, or anyone at or connected with the school.
- Use social networking sites responsibly and ensure that neither their personal nor professional reputation, nor the school's reputation is compromised by inappropriate postings.

Potential and Actual Breaches of the Code of Conduct

In instances where there has been a breach of the above Code of Conduct, the following will apply:

- Use of social media will be monitored annually and any breaches of this code will be investigated. Where it is found that there has been a breach of the policy this may result in action being taken under the Disciplinary Procedure. A breach of this policy will be considered to be a serious disciplinary offence which is also contrary to the school's ethos and principles.
- The Governing Body will take appropriate action in order to protect the school's reputation and that of its staff, parents, governors, children and anyone else directly linked to the school.

Priory Facebook Page

- The Priory CE Primary School Facebook page is visible to all those who join the group. This means that any parents, carers or others may be able to view personal pages. Be sure to keep personal pages suitable for such viewing.
- To maintain personal privacy, staff are not actively encouraged to comment on the school Facebook page.

Class Dojo

Staff must ensure that only images of children where parental consent has been granted are posted on their class story. Class Dojo is to be the only medium to report on activities within class in this manner and class accounts on other media, such as Twitter, are not to be used.

Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document.

4. Policy on Mobile Devices

Introduction and Aims

At Priory CE Primary School the welfare and well-being of our pupils is paramount. The aim of the Mobile Phone Policy is to allow users to benefit from modern communication technologies, whilst promoting safe and appropriate practice through establishing clear and robust acceptable mobile user guidelines. This is achieved through balancing protection against potential misuse with the recognition that mobile phones are effective communication tools.

Personal Mobiles - Staff

- Staff are not permitted to make/receive calls/texts during contact time with children. Emergency contact should be made via the school office so that cover can be provided. This includes serious messages e.g. news of an unwell family member. It is not appropriate to take a serious call when pupils are present as they may be left in a vulnerable situation if a member of staff becomes distressed. If a member staff considers their circumstance warrants use of phone this must be agreed with the Headteacher.
- Staff should have their phones on silent or switched off and out of sight (e.g. in a drawer, handbag or pocket) during class time.
- Mobile phones should not be used in a space where children are present (e.g. classroom, playground).
- Use of phones (inc. receiving/sending texts and emails) should be limited to non-contact time when no children are present e.g. in office areas, staff room, empty classrooms.
- It is also required that staff use security measures to protect access to functions of their phone, in the form of password protection.
- When phones are used to access confidential data (school email, CPOMS etc.), further encryption is required.
- Passwords for apps/websites containing confidential data should not be saved by the device.
- Staff should not use recording equipment on their mobile phones, for example: to take recordings of children. If, however, a significant learning opportunity would be otherwise missed, staff may use them with discretion. Recordings must be downloaded to secure school networks and then removed from the personal device at the soonest opportunity.
- Legitimate recordings and photographs should be captured using school devices: cameras and iPads.
- Staff should report any usage of mobile devices that causes a safeguarding concern to the Headteacher.
- Concerns over potential data breaches should be reported to the DPO (Mr Facey).

Mobile Phones for work related purposes

We recognise that mobile phones provide a useful means of communication on offsite activities. However, staff should ensure that:

- Mobile use on these occasions is appropriate and professional.
- Mobile phones should not be used to make direct contact with parents during school trips. Where possible, all communications should be made via the school office/Class Dojo. If the trip take place outside office hours, it may be necessary to use personal phones in some circumstances.
- Where parents are accompanying trips, they are informed not to make contact with other parents (via calls, text, email or social networking) during the trip or use their phone to take photographs of children.
- Images or videos from school trips should not be posted on personal social media accounts**,** due to potential safeguarding implications.

Other Devices

Through the course of teaching, staff will require some pieces of equipment to be removed from the premises. Laptops, Hudls, iPads and other items can be taken home but staff should ensure that:

- Items are password protected and encrypted.
- Best security measures are in place (storage in car boots, not left visible in homes etc.) to reduce the chance of theft or damage.

- Devices should only be used for school related business. The use of devices for other means opens the possibility of security issues or viruses.
- Family members are prohibited from using school equipment (laptops, iPads, Hudls etc.) for personal reasons.
- Where personal devices are used for work reasons, documents and data must be encrypted with a password and, where possible, individual logins used.
- Staff are only to use encrypted USB devices and hard drives, or USB devices provided by school to store school data and documents.

Personal Mobiles/Smart Watches – Pupils

We recognise that mobile phones and smart watches are part of everyday life for many children and that they can play an important role in helping pupils to feel safe and secure. However, we also recognise that they can prove a distraction in school and can provide a means of bullying or intimidating others. Therefore:

- The phone/watch must be handed in, switched off, to the teacher first thing in the morning and collected from them by the child at home time (the phone is left at the owner's own risk).
- Mobile phones/watches brought to school without permission will be confiscated and returned at the end of the day.
- Where mobile phones/watches are used in or out of school to bully or intimidate others, the then the head teacher does have the power to intervene 'to such an extent as it is reasonable to regulate the behaviour of pupils when they are off the school site' - refer to Anti-Bullying Policy.

Volunteers, Visitors, Governors and Contractors

All Volunteers, Visitors, Governors and Contractors are expected to follow our mobile phone policy as it relates to adults whilst on the premises. On arrival, such visitors will be informed of our expectations around the use of mobile phones.

Parents

While we would prefer parents not to use their mobile phones while at school, we recognise that this would be impossible to regulate and that many parents see their phones as essential means of communication at all times. We therefore ask that parents' usage of mobile phones, whilst on the school site is *courteous* and *appropriate* to the school environment.

5. Staff Acceptable Use Policy

Staff ICT Acceptable Use Statement

Staff should sign and have a copy of the Acceptable Use Statement. In signing, staff accept that the school can monitor network and Internet use to help ensure staff and pupil safety. The school's E-safety policy should be consulted for further information and clarification.

1. The information and communication technology and related systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.

2. I will ensure that my information systems use will always be compatible with my professional role.

3. I understand that my information systems may not be used for private purposes, without specific permission from the Headteacher.

4. I understand that the school may monitor my information systems and Internet use to ensure policy compliance.

5. I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.

6. I will not install any software or hardware without permission.

7. I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.

8. I will respect copyright and intellectual property rights.

9. I will report any incidents of concern regarding children's safety to the school E-safety Coordinator (Mr Aked) or the Designated Child Protection Coordinator (Miss Keen).

10. I will ensure that any electronic communications with pupils are compatible with my professional role.

11. I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Technology and Communication Acceptable Use Statement.

Signed: ……

Date: ……

Accepted for school by: ……

Date: ……

6. Child Acceptable Use Policy

Priory E-safety Agreement

Pupil Agreement

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

Priory CE Primary School E-Safety Rules:

1. NEVER GIVE YOUR ADDRESS OR NAME TO STRANGERS ON THE INTERNET.
2. Do not eat or drink when working on ICT equipment.
3. Personal ICT equipment, including mobile phones and smart watches, should be handed to the class teacher at the beginning of the day and returned at the end of the school day.
4. Ensure that you stay in your seat to avoid tripping over wires.
5. Only access the internet for the task that you have been given
6. Usage of the computers will be monitored by the Computing Coordinator using forensic software. Only school appropriate content should be viewed. The Headteacher will be made aware of any inappropriate use that is reported.
7. Carry all laptops with both hands. No more than 2 laptops to be carried at once.
8. Only sign on with your own log-in details unless working in a group/pair. Keep your own password safe
9. Only send emails to school email accounts (@prioryceprimary.org), unless prior permission is given by a teacher.
10. Social networking sites are banned in school and filters are used to block access to these sites.
11. Cyber-bullying is not tolerated and will be dealt with by school leaders.

Pupil: …… Class: ……

Pupil's Agreement

- I have read and I understand the school E-Safety Rules (below)
- I will use the computer, network, iPads, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access is monitored for inappropriate use.
- I understand that this agreement also covers my use of the internet and electronic devices belonging to school.

Signed (where appropriate): …… Date: ……

Priory ICT Safety Rules

1. NEVER GIVE ANY PERSONAL INFORMATION TO STRANGERS ON THE INTERNET.

2.No eating or drinking.

3. Stay in your seat.

4. Carry all laptops with both hands. No more than 1 laptop to be carried at once.

5. Only use your own log-in and never tell anyone your password.

6. No social networking in school.

7. No Cyber-bullying.

Priory ICT Safety Rules

1. NEVER GIVE YOUR ADDRESS OR NAME TO STRANGERS ON THE INTERNET.
2. Do not eat or drink when working on ICT equipment.
3. Personal ICT equipment should be handed to the class teacher at the beginning of the day and returned at the end of the school day.
4. Ensure that you stay in your seat to avoid tripping over wires.
5. Only access the internet for the task that you have been given.
6. Usage of the computers will be monitored by the Computing Coordinator using forensic software. Only school appropriate content should be viewed. The Headteacher will be made aware of any inappropriate use that is reported.Carry all laptops with both hands. No more than 2 laptops to be carried at once.
7. Only sign on with your own log-in details unless working in a group/pair. Keep your own password safe
8. Only send emails to @priorycacademy.org accounts unless permission is given by a teacher.
9. Social networking sites are banned in school and filters are used to block access to these sites.
10. Cyber-bullying is not tolerated and will be dealt with by Miss Keen and other senior leaders.




7. Parent Acceptable Use Policy

Parent/Carer Acceptable Use Policy Agreement

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. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *students/pupils* will have good access to ICT to enhance their learning and will, in return, expect the *students/pupils* to agree to be responsible users. Children are required to agree to their own acceptable use policy when they log-in to the school network, using the school ICT equipment.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

- As the parent/carer of the students/pupils named below, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

- I know that my son/daughter has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems.

- I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

- I understand that my son's/daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Pupil Name/s: ……

Parent/Carer Name: ……..

Signed: ……

Date: ……

8. E-Safety Curriculum

E-Safety Curriculum Aims

Priory's E-Safety Curriculum is built around the principles laid out in Education for a Connected. It enables the development of teaching and learning as well as guidance to support children and young people to live knowledgeably, responsibly and safely in a digital world.

It focuses specifically on eight different aspects of online education:

1. Self-image and Identity
2. Online relationships
3. Online reputation
4. Online bullying
5. Managing online information
6. Health, wellbeing and lifestyle
7. Privacy and security
8. Copyright and ownership

The framework aims to support and broaden the provision of online safety education, so that it is empowering, builds resilience and effects positive culture change. The objectives promote the development of safe and appropriate long term behaviours, and support educators in shaping the culture within their setting and beyond.' (Education For a Connected World – UKCCIS 2018)

Lessons addressing these objectives are to be taught through all stages in the school to ensure a progressive and thorough E-Safety Curriculum, equipping children with the skills and understanding to keep safe in a digital environment.

Scheme of Work Overview

Self-image and identity

This strand explores the differences between online and offline identity beginning with self-awareness, shaping online identities and how media impacts on gender and stereotypes. It identifies effective routes for reporting and support and explores the impact of online technologies on self-image and behaviour.

Online relationships

This strand explores how technology shapes communication styles and identifies strategies for positive relationships in online communities. It offers opportunities to discuss relationships and behaviours that may lead to harm and how positive online interaction can empower and amplify voice.

Online reputation

This strand explores the concept of reputation and how others may use online information to make judgements. It offers opportunities to develop strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles.

Online bullying

This strand explores bullying and other online aggression and how technology impacts those issues. It offers strategies for effective reporting and intervention and considers how bullying and other aggressive behaviour relates to legislation.

Managing online information

This strand explores how online information is found, viewed and interpreted. It offers strategies for effective searching, critical evaluation and ethical publishing.

Health, well-being and lifestyle

This strand explores the impact that technology has on health, well-being and lifestyle. It also includes understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them.

Privacy and security

This strand explores how personal online information can be used, stored, processed and shared. It offers both behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise.

Copyright and ownership

This strand explores the concept of ownership of online content. It explores strategies for protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution.

9. Links to Other Policies

- Child Protection and Safeguarding
- Behaviour
- Anti-bullying
- PSHE
- Data Protection
- Use of devices

10. Monitoring and Review

All staff are expected to ensure this policy is implemented and to have high expectations of pupils.

The Senior Leadership Team and Governing Body are responsible for monitoring the implementation and effectiveness of this policy. It will be reviewed every two years or earlier if necessary.

Policy Author: John Aked

Policy Approved By: Full Governing Board

Date Approved: June 2021

Date of Review: June 2022