Online Safety Policy

This policy applies to all pupils attending BPS. The school will ensure that all members of the school community are aware of the Acceptable Use and Online Safety policy and the implications for the individual. It should be read in conjunction with the following policies.

School Aims	Health and Safety Policy and Data Protection Policy
Safeguarding and Child Protection Policy	Positive Behaviour Policy & Anti-Bullying Policy
Acceptable Use of ICT – Pupil and Staff	PSHEE Policy

Sophie Hughes (SLT) is the Designated Safeguarding Lead (DSL) with responsible for online safety

Useful References

- Teaching Online Safety in School (DfE)
- Harmful online challenges and online Hoaxes
- Education for a Connected World (UKCIS)
- Sharing nudes and semi-nudes: advice for education settings working with children and young people (UKCIS)
- Indecent images of children: guidance for young people
- Cyberbullying: understand, prevent and respond (Childnet)
- Cyberbullying: advice for headteachers and school staff (DfE)
- Behaviour and Discipline in Schools- A guide for Headteachers and school staff
- ISI Handbook for the Inspection of Schools - Commentary on the Regulatory Requirements September 2021
- Keeping children safe in education; Statutory guidance for schools and colleges; September 2021
- Communications Act 2003
- Computer Misuse Act 1990
- Human Rights Act 1998
- Malicious Communications Act 1988:
- Telecommunications Act 1984:
- Copyright, Designs and Patents Act 1988
- The Data Protection Act 2018:
- UK General Data Protection Regulation (UK GDPR):
- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1978:
- Protection from Harassment Sct 1997:
- Public Order Act 1986:
- Racial and religious hatred Act 2006:
- Sexual Offences Act 2003:
- Equality ct 2010:

Contents

Policy Dissemination and Review

This policy will be available to parents via the school website and information will be shared throughout the year via the school bulletin. Staff will be familiar will the policy through termly INSET meetings as part of the safeguarding updates and in weekly briefings where necessary. This policy will be formally reviewed each year by the eSafety officer and updated as an ongoing process as required. The policy will be reviewed by the Governor safeguarding subcommittee on an annual basis.

Date of update	(U) Updated (R) Reviewed by	How was updated disseminated	Parents informed	Policy on website	Governor review
Sept 2016	C. Corrigan (U)	Staff briefing – email – all staff to familiarise and action	Yes	Yes	
Oct 2016	H. Gee (R)				
Feb 2017	H. Gee (U)	Staff Briefing	Yes	Yes	
Jan 2019	C. Corrigan (U)	Staff briefing – email to all staff to familiarise and action	Yes	Yes	
Jan 2020	H.Gee (U)	As above		Yes	
Jan 2021	H.Gee (R)	Teams link		Yes	
Mar2022	H. Gee (u)	Staff briefing	Yes	Yes	Yes
May 2022	H. Gee	Staff briefing & online safety training			

Latest Updates
Parents must be informed about online filtering systems during periods of online learning
Parents will be made aware of the tasks pupils are asked to undertake online, what websites they may be required to access and who they are contacting from school.
Updated links, making wider use of guidance

Introduction

At BPS we believe that ICT is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. We therefore need to build in the use of these technologies in order to provide our pupils with the skills to access lifelong learning and employment.

We are aware that raising the profile of digital learning in our school means that we must have a robust strategic plan which ensures that our pupils are able to experience all that is on offer within a safe, structured environment. This policy sets out the safety expectations of staff, parents and pupils, in respect to the use of the Internet, e-mail, messaging systems and related technologies provided by the school, and to all users accessing these services within the school environment and from home.

Purpose

This policy aims to set general principles users should apply when using the services at the school, but this guidance cannot and does not attempt to cover every possible situation. The purpose of the online safety policy is to:

- Safeguard and protect all members of the school's community online
- Identify approaches to educate and raise awareness of online safety throughout the community
- Enable all staff to work safely and responsibly, to model positive behaviour online and to manage professional standards and practice when using technology
- Identify clear procedures to use when responding to online safety concerns.

Introduction to online safety

Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is important to recognise the constant and fast passed evolution of ICT within our society as a whole as the ease of access our pupils have to ICT have outside school. Children have access to many technologies:

- Websites
- Apps
- Virtual Learning Environments
- Email
- Instant messaging and chat rooms
- Social media such as Facebook, Twitter
- Mobil/smart phones with text, video and web functionality
- Smart watches
- Other mobile devises including tablets and gaming devises
- Learning platforms and virtual learning environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video and radio/smart TV

Whilst exciting and beneficial both in and out of the context of education. Much ICT, particularly web-based resources are challenging to police, therefore all users need to be aware of the range of risks associated with use of these internet technologies and that some have age restrictions above the age of our pupils (13 years in most cases).

At BPS we understand the responsibility to educate our staff, parents and pupils about online safety issues; informing all stakeholders about the most up to date guidance available through staff training, parent workshops and for pupils, through themed days/weeks, assemblies/form sessions and the curriculum. In addition to enabling them to learn safety issues we must teach them the appropriate behaviours and critical thinking to enable them to remain safe and legal when using the internet and related technologies.

We hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners. Everybody in school has a shared responsibility to secure any sensitive information used in their professional duties and even staff who are not directly involved in data handling are made aware of the risks and threats and how to minimise them.

Both in this policy and the Acceptable Use Agreement (for Staff, Governors, regular visitors and pupils) are inclusive of both fixed and mobile internet technologies provided by the school (such as PS's, laptops, mobile devices, webcams, whiteboards etc) and any personal device of this nature that is used or can be used for work purpose.

Roles and Responsibilities

All members of the community have important roles and responsibilities to play with regard to online safety:

<u>The Headmistress</u>:

Has overall responsibility for online safety provision

- Ensures that online safety is viewed as a safeguarding issue and that practice is in line with national recommendations and requirements
- Ensures the school follows policies and practices regarding online safety (including the Acceptable Use Agreements), information security and data protection
- Ensures that online safety is embedded within the whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety
- Supports the DSL by ensuring they have sufficient training, time, support and resources to fulfil their responsibilities
- Ensures that all staff receive regular, up to date and appropriate online safety training
- Is aware of what to do in the event of a serious online safety incident, and will ensure that there are robust reporting channels for online safety concerns, including internal and national support
- Receives regular reports from the DSL on online safety
- Ensures that online safety practice is audited and evaluated regularly in order to identify strengths and areas for improvement.

The Designated Safeguarding Lead (working with the DDSL):

- Takes day to day responsibility for online safety
- Promotes an awareness of and commitment to online safety throughout the school community
- Acts as the named point of contact on all online safety issues, and liaises with other members of staff or other agencies, as appropriate
- Keeps the online safety component of the curriculum under review, in order to ensure that it remains up to date and relevant to pupils
- Facilitates training and advice for all staff, keeping colleagues informed of current research, legislation and trends regarding online safety and communicating this to the school community, as appropriate
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident (in or out of school)
- Monitors pupil internet usage, taking action where required
- Maintains the online safety incident log and record of actions taken, and reviews the log periodically to identify gaps and trends
- Reports regularly to the Headmistress and SLT on the incident log, internet monitoring, current issues, developments in legislation etc.
- Ensure Governors are updated and that all Governors have an understanding of the issues and strategies at the school in relation to local and national guidelines and advice.

Staff managing the technical environment (Network Manager and Bursar):

- Apply appropriate technical and procedural controls to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised
- Keep up to date with the school's online safety policy and technical information in order to carry out their online safety role effectively and to inform and update others as relevant
- Provide technical support to the DSL and leadership team in the implementation of online safety procedures
- Ensure that the school's filtering policy is applied and updated on a regular basis, and oversees the school's monitoring system
- Report any filtering breaches or other online safety issues to the DSL, Head, GDST and other bodies, as appropriate
- Ensure that any safeguarding concerns are reported to the DSL, in accordance with the school's safeguarding procedures
- Ensure parents are informed about online filtering systems during periods of online learning

All school staff (including support workers and volunteers):

- Read, adhere to and help promote the online safety policy, Acceptable Use Agreements and other relevant school policies and guidance
- Take responsibility for the security of school systems and the data they use, or have access to
- Model safe, responsible and professional behaviours in their own use of technology
- Embed online safety in their teaching and other school activities
- Supervise, guide and monitor pupils carefully when engaged in activities involving online technology (including extra-curricular and extended school activities if relevant)
- Have an up to date awareness of a range of online safety issues and how they may be experienced by the children in their care
- Identify online safety concerns and take appropriate action by reporting to the DSL
- Know when and how to escalate online safety issues
- Take personal responsibility for professional development in this area.
- Ensure parents are made aware of the tasks pupils are asked to undertake online, what websites they may be required to access and who they are contacting from school

Pupils (at a level that is appropriate to their individual age, ability and vulnerabilities):

- Engage in age-appropriate online safety education opportunities
- Read and adhere to the school Acceptable Use Agreement
- Respect the feelings and rights of others both on and offline, in and out of school
- Take responsibility for keeping themselves and others safe online
- Report to a trusted adult, if there is a concern online.

Parents:

- Read the school Acceptable Use Agreements and encourage their children to adhere to them
- Support the school in online safety approaches by discussing online safety issues with their children and reinforcing appropriate, safe online behaviours at home
- Model safe and appropriate use of technology and social media, including seeking permission before taking and sharing digital images of pupils other than their own children
- Identify changes in behaviour that could indicate that their child is at risk of harm online
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online

- Use school systems, such as learning platforms, and other network resources, safely and appropriately
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

External groups:
- Any external individual/organisation must sign an Acceptable Use Agreement prior to being given individual access to the school network.

Education and Engagement

The school curriculum includes age-appropriate lessons and activities on online safety for all pupils, intended to raise awareness, build resilience and promote safe and responsible internet use by:
- Ensuring education regarding safe and responsible use precedes internet access
- Including online safety across the curriculum, including the Personal Social and Health Education, Relationships and Sex Education and Computing programmes of study, covering use both at school and home
- Reinforcing online safety messages whenever technology or the internet is in use
- Ensuring that the needs of pupils considered to be more vulnerable online, such as those with SEND or mental health needs, are met appropriately
- Using support, such as peer education approaches and external visitors, to complement online safety education in the curriculum
- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation
- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Teaching pupils to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Supporting pupils in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision making
- The school will support pupils to read and understand the Acceptable Use Agreement in a way which suits their age and ability by:
    - Discussing the AUA and its implications, and reinforcing the principles via display, classroom discussion etc.
    - Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation
    - Recognising positive use of technology by pupils.

Training and engagement with staff

The school will:
- Provide and discuss the Online Safety Policy and staff Acceptable Use Agreement with all members of staff as part of induction
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community

Awareness and engagement with parents and carers

Parents have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies. The school will build a partnership approach to online safety with parents and carers by:
- providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such Transition meetings, Coffee Mornings, Parent Voice sessions Lead by the Headmistress.
- drawing parents' attention to the school online safety policy and expectations in the weekly Bulletin and newsletters and via social media
- requiring parents to read the pupil Acceptable Use Agreement and discuss its implications with their children

Protecting Children

The internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. The school will:

- regularly review the methods used to identify, assess and minimise online risks
- examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted
- ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material
- ensure, through online safety education and the school AUAs, that pupils know that the school's expectations regarding safe and appropriate behaviour online apply whether the school's networks are used or not.

Safer Use of Technology

Classroom Use

- The school uses a wide range of technology. This includes access to:
    - computers, laptops and other digital devices
    - internet which may include search engines and educational websites
    - learning platforms
    - cloud services and storage
    - email and messaging
    - digital cameras, web cams and video cameras
- Supervision of pupils will be appropriate to their age and ability
- All school-owned devices should be used in accordance with the school's AUAs and with appropriate safety and security measures in place.
- Members of staff should always check websites, tools and apps for suitability before use in the classroom or recommending for use at home
- Staff and pupils should consider copyright law before using internet-derived materials (and where appropriate comply with licence terms and/or acknowledge the source of information)

Appropriate Filtering

Web filtering at the school is via a firewall supplied by Wave9 and Sophos. Web filter categories are agreed by the Phase Leaders. Requests for individual blocking or allowing of sites can be made by a member of staff and checked by the network manager. If they are unsure on a particular site, they will consult with a designated safeguarding person.

At BPS we follow guidelines from the UK Safer Internet Centre in order to comply with Keeping Children Safe in Education (KCSIE). They state:

Inappropriate Online Content Recognising that no filter can guarantee to be 100% effective, schools should be satisfied that their filtering system manages the following content (and web search)

1. Discrimination: Promotes the unjust or prejudicial treatment of people on the grounds of the protected characteristics listed in the Equality Act 2010

2. Drugs / Substance abuse: displays or promotes the illegal use of drugs or substances

3. Extremism: promotes terrorism and terrorist ideologies, violence or intolerance

4. Malware / Hacking: promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content

5. Pornography: displays sexual acts or explicit images

6. Piracy and copyright theft: includes illegal provision of copyrighted material

7. Self-Harm: promotes or displays deliberate self-harm (including suicide and eating disorders)

8. Violence: Displays or promotes the use of physical force intended to hurt or kill

What we do:

Discrimination: We block the Discrimination category for all pupils. Drugs / Substance abuse: We block the Drug Abuse category for all pupils. Extremism: We block the Extremist Groups category for all pupils.
Malware / Hacking: We block the Proxy Avoidance and Hacking category for all pupils.
Pornography: We block the Pornography category for all pupils.
Piracy and copyright theft: We block the Plagiarism category for all pupils.

Self Harm: There is no specific category for Self Harm in the firewall but all abuse categories are blocked for all pupils.
Violence: We block the Explicit Violence category for all pupils.

Dealing with Filtering breaches

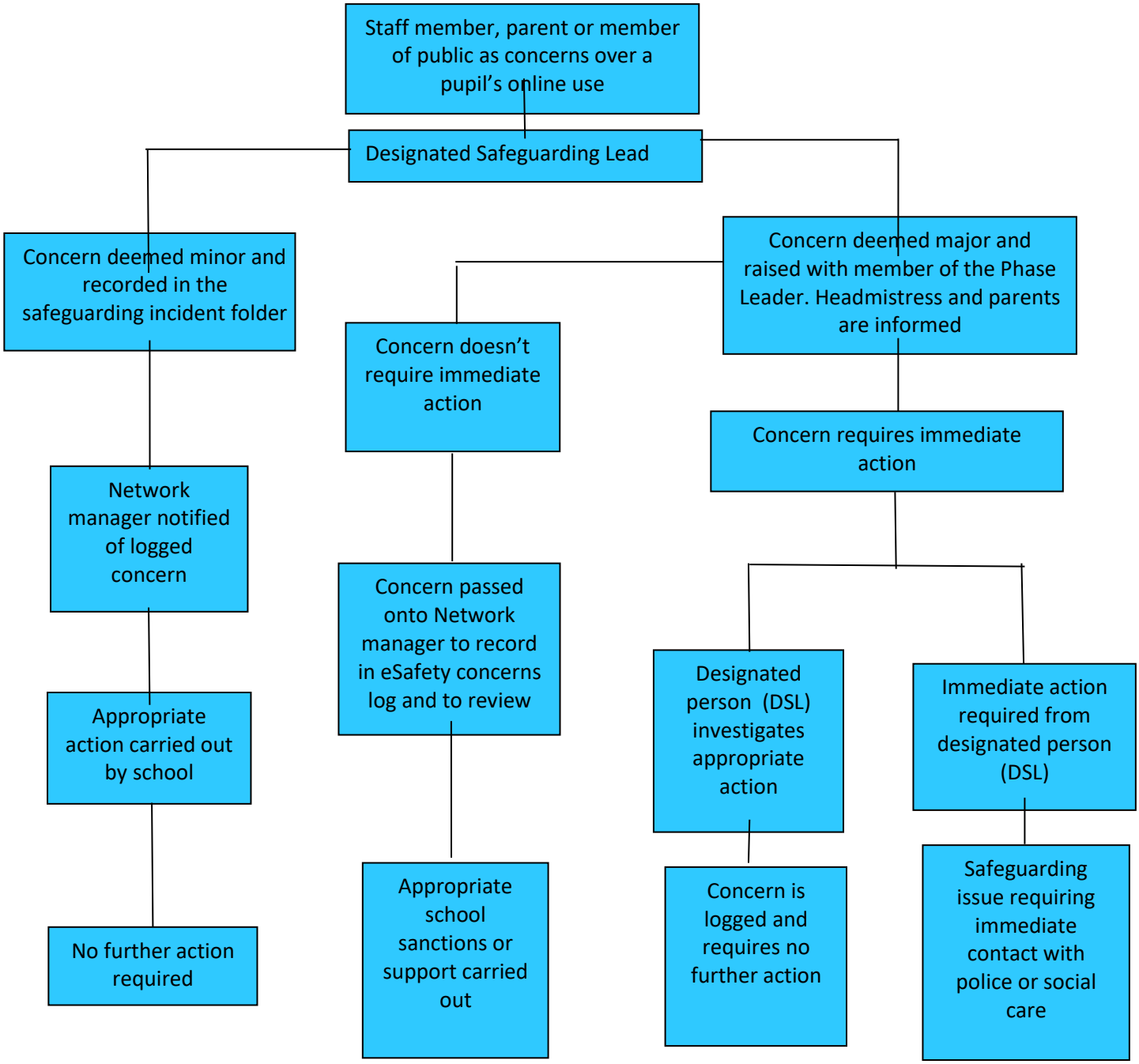
The school recognises that despite employing safety procedures, in some circumstances, the Internet may give children access to undesirable information or images. The school has a clear procedure for reporting filtering breaches which pupils are regularly reminded of:

1. They must immediately turn off the screen.
2. Report immediately to the teacher or supervising adult. The member of staff will report the concern (including the URL of the site if possible) to the DSL to the Headmistress and Network Manager
3. The breach will be recorded and escalated as appropriate
4. Pupils will refrain from describing or encouraging others from accessing the site either directly or through a search engine.
5. Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as Internet Watch Foundation (IWF), the Police or Child Exploitation and Online Protection (CEOP).

Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns
- Incidents will be managed depending on their nature and severity, according to the relevant school policies
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes in policy or practice as required
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Trafford Safeguarding Board or ISA.
- Where there is suspicion that illegal activity has taken place, the school will contact the Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with the Police and/or the Local Authority first, to ensure that potential investigations are not compromised.

Dealing with Concerns



Managing Personal Data

Online Personal data will be collected, processed, stored and transferred in accordance with the General Data Protection Regulations and the GDST's Privacy Notices. Full information can be found in the school's Data Protection Policy.

Emails

Curriculum activities that involve the use of e-mail will be through the use of Purple Mash, the Pupil Portal (Engage) and/or class or group webmail accounts that are controlled by the school. All email communications sent by members of staff that relate to the school will be through authorised, school controlled webmail accounts. The use of individual pupil personal accounts will not be permitted through the school system. Any e-mail sent to an external account will be authorised by the school, before sending, following the same

procedure used for letters written on school headed notepaper. Pupils will never reveal personal details of any member of the school community in e-mail communications.

Mobile Phones, Social Media and Portable Devices – see Acceptable Use of ICT

Pupil use of online messaging is only allowed through their Pupil Portal as this can be supervised or monitored in a way that will support safety of the pupils. Personal use of mobile phones by staff is not permitted during lessons or formal school time. Staff must ensure that personal devices are switched off during lessons, but they are permitted to use these devices (during breaks and non-contact time) away from children in the Staff Workroom. Parents and Visitors to the school are not permitted to use mobile phones whilst on the premises, in line with our safeguarding policy.

The School Website

The school website is maintained and kept up to date. The headmistress ensures that the content is accurate and appropriate to the needs of the school community. No personal information about any member of the school community will be published on the website. Written permission from parents or carers will be obtained before photographs of pupils or pupil names are published on the website. Only first names of pupils will be published and these will never be published in conjunction with photographs. Any photographs published will not allow individual pupils to be identified.

Consent Forms

A consent form, which covers permission to access the Internet, will be issued to parents and carers. This will contain the acceptable use guidelines and details of the school eSafety policy. Parents will be required to sign the consent form and where appropriate pupils will also be required to sign the Acceptable Use of ICT agreement. Pupils are informed that internet use will be monitored. Pupil access may be withdrawn if the acceptable use guidelines are not adhered to.

All members of staff including teachers, supply staff, classroom assistants and support staff, will be provided with access to a copy of the school eSafety policy. All staff sign a copy of the Acceptable use of ICT before using any internet access or resources in school. Staff will be made aware that internet traffic can be monitored and traced to the individual user and professional conduct is essential. Staff development in safe and responsible internet use will be provided as part of the continuing professional development programme.

Monitoring and Reporting

The eSafety Officer will ensure that the eSafety Policy is implemented and compliance with the policy monitored. Staff and pupils should be aware that some material available on the Internet is inappropriate for specific age groups and could therefore cause risks of harm. Every teacher needs to be aware of the risks posed by online activity, including that of extremist and terrorist groups.

Methods to identify, assess and minimise risks will be reviewed regularly. The school will take all reasonable precautions to ensure that pupils access only appropriate material. However, due to the nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Where unsuitable content is encountered, staff and pupils should follow the school procedures for such events. Unsuitable URL addresses will be reported through the IT Manager. Pupils must report unsuitable material, including e-mail content, immediately to a teacher. The teacher will then ensure that the reporting procedures are followed. Parents will be informed of such incidents sensitively to avoid undue distress.

Where incidents occur due to non-compliance with the school eSafety policy these will be reported to the ICT Manager and if necessary, the eSafety Officer. Any issues relating to staff misuse must be referred to the

Headmistress. Should it become necessary to prohibit the use of internet resources for a pupil, then parents or carers will be involved so that a partnership approach can be used to resolve any issues. This could include practical sessions and suggestions for safe Internet use at home.

Appendix 1

Measures Taken

We have created a safe digital learning environment consisting of the following elements:

- Web Filtering - Web filtering is handled by our firewall, it detects the user or device that is logged in and applies the appropriate level of filtering. The categories that are blocked are discussed with the SLT

- Web Monitoring – Pupils are not allowed to access IT equipment without there being a member of staff present

- Safesearch - Safesearch facilities have been enabled for the major search engines and streaming media sites where possible. SSL (Secure Sockets Layer) Inspection is also enforced for pupil traffic which allows secure content to be inspected to detect search terms.

- Port and Service Restrictions - Access has been given to only essential ports and services through the firewall.

- Mobile Device Management (MDM) – whilst no MDM software is deployed network level filtering is applied and is not reliant on any software on user devices whilst at school. Staff devices may have be used to work from home, but are never accessed by pupils.

Appendix 2

Websites for Pupils and Parents

KidSmart - Learn more about the Internet and how to be a SMART surfer

ThinkUKnow - Advice on online safety

CBBC Stay Safe - ESafety games and songs

Childnet - Working to make the Internet a safe place for children

DigiDuck's Big Decision - A story about online friendship and making the right decisions (KS1)

Adventures of Smartie The Penguin -A story about asking for help when using the Internet (KS1)

Digizen - Become a responsible digital citizen

The Adventures of Kara, Winston and the SMART Crew

Safe Network - Guidance on helping keep children safe online

The Parents' and Carers' guide to using the Internet

CEOP YouTube Channel (for Parents/Carers)

Digital Family - o2

Keep Safe Online - Cyberbullying

Keep Safe Online - Glossary of Terms

- Action Fraud: www.actionfraud.police.uk
- CEOP:
    - www.thinkuknow.co.uk
    - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  o ChildLine: www.childline.org.uk
  o Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
    - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
    - Telephone helpline: 0844 381 4772

Move to top of document