Online Safety Policy

September, 2019

Pheasey Park Farm Primary School and Children's Centre

Online Safety Policy

Introduction

Today's children are citizens of a digital world. In their daily lives the use of the internet and digital technologies represents a seamless extension of the physical world. Their emotional lives and their development are bound up in the use of these technologies. In contrast to many adults for whom these technologies are additional tools to be used for specific tasks, many of today's children do not even notice they are using these technologies. As online content, social networking and instant messaging converge with mobile technology to produce lives which are always 'on', any line which may have existed between being online and offline is disintegrating.

The Internet is a fantastic resource that children are using as a normal part of everyday life. However, in the same way that we do not allow them to wander around the world by themselves or talk to strangers, it is equally important that we protect them when they are exploring the virtual world. As a school we have set up the School Launchpad which is a safe, secure environment for children to use both in school and at home. Within the Launchpad there are educational resources and games, eBooks and useful Online Safety links to websites. During the weekly ICT Assemblies children are informed about the dangers of the internet. Establishing ways of discussing internet safety, setting guidelines and strategies for when things go wrong, has never been more important.

Online Safety encompasses Internet technologies and electronic communications such as mobile phones, tablets and computers as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. We need to equip children with the knowledge to navigate the online world safely.

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and children; encouraged by education and made explicit through published policies.
- Sound implementation of online Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Walsall network, including the effective management of filtering systems.
- Compliance with Data Protection, GDPR and ICO Regulations.

Keeping Children Safe in Education (Latest Version)

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk: • content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

• contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

• conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

School Procedures

- The Digital Learning Leader is the appointed person to co-ordinate Online Safety.
- The Online Safety Policy has been agreed by senior management and approved by governors.
- The Online Safety Policy and its implementation will be reviewed annually.
- Ongoing staff Online Safety training (making staff aware of the different social networks and the appropriate terminology.
- Use of CEOP (Child Exploitation and Online Protection Centre) as an online reporting mechanism.
- Online Safety is covered in staff meetings, parent workshops and ICT assemblies.

- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Roles and Responsibilities

Governors:
The role of the online Safety governor will include:
- Regular meetings with the Online Safety co-ordinator
- Regular monitoring of Online Safety incident logs
- Regular monitoring of filtering
- Reporting back at Governor meetings
- Representing governors at the Online Safety committee meetings

Head teacher:
- The head teacher has a duty of care for ensuring the safety (including Online Safety) of members of the school community, though the day to day responsibility for online Safety will be delegated to the Online Safety Co-ordinator
- The head teacher and at least another member of the SMT should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff
- The head teacher is responsible for ensuring that the Online Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their online Safety roles and to train other colleagues
- The head teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online Safety monitoring role

Online Safety Co-ordinator:
The role of the Online Safety Co-ordinator will include:
- Responsibility for online Safety issues as well as reviewing the school online Safety policies
- Ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place
- Provide training and advice for staff
- Liaise with external agencies
- Receives reports of Online Safety incidents and create a log of incidents to inform future online Safety developments
- Meets regularly with the Online Safety Governor
- Reports regularly to the SMT
- Providing advice and guidance for parents
- Chair the Online Safety Committee meetings

ICT Technician (Joskos Solutions):

The role of the technical staff will include:

- Ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- Ensuring that the school meets required online Safety technical requirements and any Local Authority / other relevant body Online Safety Policy / Guidance that may apply.
- Ensuring that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- Making sure they have an up to date awareness of online Safety matters and of the current Online Safety policy and practices
- Ensuring that they have read, understood and signed the Staff Acceptable Use Policy
- Ensuring that they report any suspected misuse or problem to the Head teacher/Online Safety Co-ordinator for investigation/action/sanction

Teaching and Support Staff:

The role of the teaching and support staff will include:

- Having an up to date awareness of Online Safety matters and of the current school online Safety policy and practices
- Ensuring they have read, understood and signed the Staff Acceptable Use Policy
- Reporting any suspected misuse or problem to the Head teacher/Online Safety Co-ordinator for investigation/ action/sanction
- All digital communications with staff/students/pupils/parents/carers should be on a professional level and only carried out using official school systems
- Online Safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the Online Safety and acceptable use policies
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Monitor the use of digital technologies, mobile devices, tablets, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and processes in place for dealing with any unsuitable material that is found in internet searches
- If staff or pupils discover unsuitable sites, the URL (address) time, date and content will be immediately reported to the Online Safety Co-Ordinator.
- Staff should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- Staff will have access to all Online Safety assembly PowerPoints and resources.

Pupils:

- Are responsible for using the school digital technology systems in accordance with the Student/Pupil Acceptable Use Policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. The school will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- Should understand the importance of adopting good online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be taught about sharing imagery (photographs/videos) that may cause embarrassment, pupils will need to understand what the outcomes of this action will be. This is in preparation for KS3 when pupils will be warned against 'Sexting' the sharing of youth produced sexual imagery.
- Pupils using the internet will be supervised within the class by an adult. Internet access will be granted to a whole class as part of a scheme of work. There may be situations when pupils have freedom for research using an appropriate search engine or are directed to a specific approved online resource. Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught how to evaluate Internet content. They should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- Pupils will participate in weekly ICT assemblies with a focus on Online Safety, they will be questioned about safety issues throughout the year, both in Key Stage 1 and Key Stage 2.
- Pupils will have an opportunity to design Online Safety posters demonstrating their knowledge. Winning entries will be displayed around the school.
- Age appropriate Online Safety posters and information will be displayed with classrooms.

Online Safety Committee
Represented by Digital Learning Leader, SMT, Safeguarding lead, Online Safety Governor, Teaching Staff representative, Technician.
- Discuss current Online Safety issues or threats.
- Review policies and procedures.
- Evaluate teaching of online safety.
- Discuss emerging technologies.
- Consult Stakeholders including pupils

Teaching and learning
Curriculum – Education Technology is embedded throughout the curriculum. Technology is also used for assessment and administrative purposes.

Why is Internet use important?
- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries;
- Educational and cultural exchanges between pupils worldwide;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across networks of schools, support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data.
- Access to learning wherever and whenever convenient.
- Access to school learning platform.

How can Internet use enhance learning?

- The school's Internet access will be designed to enhance and extend education.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.

Managing Information Systems

How will information systems security be maintained?

- The security of the school information systems, systems capacity, security and users will be reviewed regularly.
- The school uses broadband with firewall and filters.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Head teacher and external agencies.
- Personal data sent over the Internet or taken off site will be encrypted. USB pens will be password protected.
- Portable media may not be used without specific permission followed by an anti-virus/malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The Digital Learning Leader will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.
- Computer use is monitored by the and SMT through security software which logs any potential misuse by any person accessing school computers on or off site.

How will E-mail be managed?

- The school uses a secure E-mail system – Office 365.
- Pupils will not be allowed to access personal e-mail accounts or chat rooms whilst in school.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- School e-mail will be used for classes communicating outside of the school to another school.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers through the office staff.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Emails sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.
- Professional E-mail communication needs to be restricted to only necessary communication.

How will published content be managed?

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The Head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website and Learning Platform will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Can pupils' images or work be published?

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Photographs or videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified, unless specified otherwise.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published on the internet. (Website, Learning Platform or External agencies.)
- Pupils work can only be published with their permission or the parents.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.
- The School will have a policy regarding the use of photographic images of children which outlines policies and procedures.

How will social networking, social media and personal publishing be managed?

- The school will control access by blocking access to social media and social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone

numbers, school attended, email addresses, full names of friends/family, specific interests and clubs etc.

- Staff wishing to use Social Media tools with pupils as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will follow the guidelines when using Social Media tools in the classroom.
- Staff official blogs or wikis should be password protected and run from the school website with approval from SMT. Members of staff are advised not to run social network spaces for pupil use on a personal basis.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding pupils use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning pupils underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school's Acceptable Use Policy and staff code of conduct.

How will filtering be managed?

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with Walsall digital team to ensure that the filtering policy is continually reviewed and improved.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School Online Safety Co-ordinator who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from SMT.
- SMT will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from external agencies.
- Video conferencing should be supervised appropriately for the pupils' age. Pupils should not answer or make a video conference call.

How are emerging technologies managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used in formal school time.
- The sending of abusive or inappropriate text messages is forbidden.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Policy.

- Video Conferencing will be appropriately supervised for the pupils' age.

How are emerging issues managed regarding Online Safety in Key Stage 3?

- Links will be created between Online Safety Coordinators in Primary and Secondary education.
- Issues that affect older pupils (KS3) will be acknowledged and addressed. Age appropriate precautions will be put into place to manage any issues in the future.
- Pupils will receive age appropriate Online Safety training regarding issues that they may come into contact with in the future.

How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to GDPR regulations.

Policy Decisions

How will Internet access be authorised?

- All staff will be given the School Online Safety Policy and its importance explained.
- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff will read and sign the 'Acceptable ICT Use Agreement' before using any school Education Technology resources.
- The Head teacher will ensure that the Online Safety Policy is implemented and compliance with the policy monitored.
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of Internet misuse will be dealt with by the Digital Learning Leader or a senior member of staff, then passed onto the Head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Advice on Online Safety will be introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet use.
- Parents and pupils will be asked to sign and return a consent form agreeing to comply with the school's Acceptable Use Policy.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- All visitors to the school who require access to the school's network or internet access will be asked to read and sign an Acceptable Use Policy.
- Pupils' access to the Internet will be under adult supervision.
- Online Safety rules will be displayed where appropriate and discussed with the pupils during ICT assemblies.
- Pupils will be informed that network and Internet use will be monitored.
- Parent's attention will be drawn to the School Online Safety Policy in newsletters, Online Safety booklet and on the School website.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

- Pupils access will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

How will risks be assessed?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit Education Technology use to establish if the Online Safety policy is adequate and that the implementation of the Online 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.

How will the school respond to any incidents of concern?

- All members of the school community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.)
- The Online Safety Coordinator will record all reported incidents and actions taken in the School online Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Child Protection Coordinator will be informed of any Online Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage Online Safety incidents in accordance with the school Behaviour Policy and Safeguarding Policies.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or Online Safety officer and escalate the concern to the Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County Online Safety Officer.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the local Online Safety officer.

How will Online Safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the Head teacher.
- All Online Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguard Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.

- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

Pupils Use of Personal Devices

- Only under exceptional circumstances will Pupil's mobile phones be allowed to be kept in the school office. (e.g. A pupil who uses public transport and needs a phone for safety during the journey, will be able to store the phone in the School Office throughout the day.)
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity unless authorised by SMT.
- Staff will be issued with a school phone where contact with pupils or parents/carers is required.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of SMT in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by SMT.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Communication Policy

How will the policy be introduced to pupils?
- All users will be informed that network and Internet use will be monitored.
- An Online Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to Online Safety education will be given where pupils are considered to be vulnerable.

How will the policy be discussed with staff?
- The Online Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.

- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- Staff who manage filtering systems or monitor technology use will be supervised by SMT and have clear procedures for reporting issues.
- The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

How will parents' support be enlisted?

- Parents' attention will be drawn to the school Online Safety Policy in newsletters, the school prospectus, the school website and ICT parent workshops.
- A partnership approach to Online Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting Online Safety at other attended events e.g. parent evenings and sports days.
- Parents will be requested to sign an E–Safety/Internet agreement as part of the Home School Agreement.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on Online Safety will be made available to parents in a variety of formats.
  Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations listed in the "Online Safety Contacts and References section".
- Tips for parents regarding internet safety are included on the website.

<u>Links with other policies</u>

Computing, Behaviour, Anti-Bullying, PSHE, Safeguarding, Data Protection, Health and Safety, Social Networking and code of conduct.

<u>Monitoring and Review</u>

This policy will be reviewed annually by the Digital Learning Leader.

Mr P Godwin
September, 2019