On-line Safeguarding policy

September 2017

Signed:

Headteacher: Alison Gibson

Signed:

On behalf of the Governing Body

Proposed Review Date: September 2018

Introduction

The e-Safety Policy is part of the School Development Plan and will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Curriculum, Data Protection and Security.

Our e-Safety Policy has been written by the I.C.T Coordinator in collaboration with the Head Teacher and Senior leaders, building on the Lancashire Children and Young Peoples' Directorate and Government guidance. It has been agreed by Farington Moss St. Paul's School's Senior Leadership Team and approved by the full Governing Body.

The school e-Safety Coordinators are the Computing Subject Leaders
The responsible member of the Governing Body is:
Safeguarding Governor/Child Protection Governor: Chair of Governors Ian Quinn
The Designated Senior Person is: Alison Gibson Head Teacher

The Deputy DSP's are: James Eccleston and Ann Oaten

Pupils interact with new technologies such as mobile phones, tablets etc and use the Internet on a daily basis, experiencing a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally place young people in danger.

E-safety covers issues relating to children and young people and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education on risks and responsibilities and is part of the "duty of care" which applies to everyone working with children.

TEACHING AND LEARNING

Why the Internet and digital communications are important:

The Internet is an essential element in 21st century 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.

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 provided by Lancashire LA.

Pupils will be taught what Internet use is acceptable and what is not and given clear guidelines for Internet use.

Pupils will be educated 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.

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Pupils will be taught the importance of cross-checking information before accepting its accuracy.

Pupils will be taught how to report unpleasant Internet content.

MANAGING INTERNET ACCESS

Information system security

School ICT systems security will be reviewed regularly with the school's ICT technician.

Virus protection will be updated regularly by the school's technician.

Security strategies will be discussed with the Local Authority and reviewed as appropriate, depending on any guidance or guidelines received. Filtering is provided by BT Light Speed.

E-mail

- Pupils may only use approved/class e-mail accounts on the school system
- Pupils must only use messaging facilities within the school approved VLE(*Virtual Learning Environment*)
- Pupils must immediately tell a teacher if they receive offensive e- mail/message
- Whole class or group e-mail addresses should be used in school
- In any electronic communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission
- Access in school to external personal e-mail accounts may be blocked
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known
- E-mail or messages sent to an external organization should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- The forwarding of chain letters is not permitted

Published Content and the School Web Site

- The contact details on the Web site will be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Content will be updated by teaching staff and teacher led T.A's

Publishing Pupil's Images and Work

- Photographs that include pupils will be selected carefully and will only be used if parents give permission.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories. (Written consent is obtained annually during data collection checking from parents regarding this)
- Work can only be published with the permission of the pupil and parents.
- The school is not responsible for third party publishing e.g. publishing details as a result of media coverage e.g. on a newspaper website.

Social Networking and Personal Publishing

- The school will block/filter access to social networking sites where possible.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Parents and carers are reminded at every school event not to post photos on any social sites.

Staff

All staff need to be made aware of the following points:

- The content on Social Network sites may be unmediated and inappropriate for certain audiences.
- If a Social Network site is used personally, details must not be shared with children and privacy settings be reviewed regularly to ensure information is not shared automatically with a wider audience than intended.
- They must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
  The content posted online should not:
  a.bring the school into disrepute
  b.lead to valid parental complaints
  c. be deemed as derogatory towards the school and/or its employees
  d. be deemed as derogatory towards pupils and/or parents and carers
  e. bring into question their appropriateness to work with children and young people.
- Adults must not communicate with children using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted. Online Communications with parents, past pupils or siblings of pupils, especially if under the age of 18 should be discouraged.
- Children must not be added as 'friends' on any Social Network site.

Infrastructure and Technology

Our school ensures that the infrastructure/network is as safe and secure as possible. We subscribe to the Lancashire Grid for Learning/CLEO Broadband Service, internet content filtering is provided by default. It is important to note that the BT Lightspeed filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service. Sophos Anti-Virus software is included in the school's subscription, but this needs to be installed on computers in school and then configured to receive regular updates. We employ a technician to ensure this security is in place and regularly updated.

Through Safeguarding training all staff are aware of the requirement to identify children who may be vulnerable to radicalisation and extremism and recognise that this risk is seen as part of the wider safeguarding duties, and is similar in nature to protecting children from other harms (eg. Drugs, gangs, neglect, sexual exploitation), whether these come from within their family or are the product of outside influences. The school is committed to the Prevent duty (Sept.15). The Prevent duty requires staff to take action when they observe behaviour of concern. Reference will be made to the statutory guidance (KCSIE September 2016 and Working together to Safeguard children and Guidance for safer working practice for those working with Children and Young People in education settings – October 2015).

Referral to the Channel programme will be made if there are concerns that an individual might be vulnerable to radicalisation. School will access LEA training and WRAP training. The local police force can be contacted for advice 101 (the non-emergency number).

The DfE has a dedicated telephone helpline (020 7340 7264) to enable staff and governors to raise concerns relating to extremism directly. Concerns can also be raised by e-mail to counter.extremism@education.gsi.gov.uk.

Children's access

Children are always supervised by an adult when accessing school equipment and online materials.
Children have personal passwords which allow them to log onto the school network, but only allows them access to the pupil drive of the server.

Adult access

Staff access the school network through personal passwords. The I.T. technician holds the administrator password. The school office system is on a different system.

Passwords

All users of the school network have a secure username and password.
The administrator password for the school network is available to the Head Teacher or other nominated senior leader and is kept in a secure place.
Staff and children are reminded of the importance of keeping passwords secure.
Staff passwords are required to be changed at regular intervals.
Passwords are expected to be of a format that is not easy to guess, eg a mixture of letters, numbers and capital and lower case letters.

Software/hardware

- We have legal ownership of all software (including apps on tablet devices)
- BT Lancashire have an up to date record of appropriate licenses for all software and who are responsible for maintaining this.
- We regularly audit equipment and software.
- IT technician controls what software is installed on school systems.

Managing the network and technical support

- Servers, wireless systems and cabling are securely located and physical access is restricted.
- All wireless devices have security enabled
- Wireless devices are accessible only through a secure password
- School has restricted access settings on tablet devices and secure password and account details are needed e.g. for downloading of apps or 'in- app' purchases
- IT technician is responsible for managing the security of our school network
- IT technician reviews the safety and security of our school network termly
- School systems are kept up to date in terms of security via the IT technician e.g. computers regularly updated with critical software updates/patches

- Users (staff, children, guests) have clearly defined access rights to our school network e.g. they have a username and password and permissions are assigned accordingly
- Staff and children are required/reminded to lock or log out of the school system when a computer/digital device is left unattended
- Teachers are allowed to download executable files or install software
- School laptops / iPads are password protected and are only to be used for professional use in school and at home. e.g lesson planning and work related use
- Network monitoring is in accordance with the Data Protection Act (1998)

Filtering and virus protection

The filtering is managed by BT Lancashire, through on sight visits and remote access to the school systems to rectify problems.
Filtering is managed by the technician and the ICT Coordinator.

Virus protection is updated by the IT technician.

Dealing with incidents

An incident log will be completed to record and monitor offences. This will be audited on a regular basis by the ICT Coordinator or other designated member of the Senior Leadership Team.

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Head Teacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). **Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence.** It is essential that correct procedures are

followed when preserving evidence to protect those investigating the incident (See Appendix 12). Always report potential illegal content to the Internet Watch Foundation (**http://www.iwf.org.uk**)
.They are licensed to investigate – schools are not!

Examples of illegal offences are:
Accessing child sexual abuse images
Accessing non-photographic child sexual abuse images
Accessing criminally obscene adult content
Incitement to racial hatred
More details regarding these categories can be found on the IWF website **http://www.iwf.org.uk**

Inappropriate use

It is more likely that our school will need to deal with incidents that involve inappropriate rather than illegal misuse. We will deal with any incidents quickly and actions are proportionate to the offence. Some examples of inappropriate incidents are listed below with suggested sanctions:

Incident	Procedure and Sanctions
Accidental access to inappropriate materials.	Minimise the webpage/turn the monitor off/click the 'Hector Protector' button. Close the laptop lid Tell a trusted adult. Enter the details in the Incident Log and report to LGfL filtering services if necessary. Persistent 'accidental' offenders may need further disciplinary action.
Using other people's logins and passwords maliciously.	Inform SLT or designated eSafety Champion. Enter the details in the Incident Log. Additional awareness raising of eSafety issues and the AUP with individual child/class. More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. Consider parent/carer involvement.
Deliberate searching for inappropriate materials.	
Bringing inappropriate electronic files from home.	
Using chats and forums in an inappropriate way.	

- SLT members are responsible for dealing with eSafety incidents.
- All staff are aware of the different types of eSafety incident and how to respond appropriately e.g. illegal or inappropriate.

- Through training, staff report safety incidents to SLT members of staff
- Children are informed of the procedures through e-safety lessons in computing and in other curriculum areas.
- Incidents are logged in the record log file
- Incidents are monitored by the Head teacher and Chair of Governors
- Application of appropriate policies eg Behaviour Management, Discipline and Child Protection policies

Reference will be made to the 'eSafety Incident/Escalation Procedures' document
(See Appendix 12) as procedure for teachers and support staff.

Acceptable Use Policy (to be read alongside Code of Conduct for school staff)

An Acceptable Use Policy is intended to ensure that all users of technology within school are responsible and are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.

School request parental permission to use ICT and access to sites

AUPs are recommended for Staff, Children and Visitors/Guests and must be signed and adhered to by users before access to technology is allowed. You may wish to consider this agreement as a partnership between parents/carers, children and the school to ensure that users are kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology must be kept in school and made available to all staff.

Our school adopted the APU's from L.E.A Appendix A,B &C

Education and training

In 21st Century society, both adults and children need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that children are taught to use technology responsibly, securely and safely, being able to recognise potential risks and knowing how to respond. They should, for example, be able to communicate safely and respectfully online, be aware of the necessity to keep personal information private, be taught how to search effectively and be discerning in their evaluation of digital content and be aware of the need to respect copyright and Intellectual Property rights.

The three main areas of eSafety risk (as mentioned by OFSTED, 2013) that our school is aware of and considers are:

Area of Risk	Example of Risk
Content: Children need to be taught that not all content is appropriate or from a reliable source.	Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse. Lifestyle websites, for example pro-anorexia/self-harm/suicide sites. Hate sites. Content validation: how to check authenticity and accuracy of online content.
Contact: Children need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	Grooming Cyberbullying in all forms Identity theft (including 'frape' - hacking Facebook profiles) and sharing passwords.
Conduct: Children need to be made aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves and others.	Privacy issues, including disclosure of personal information, digital footprint and online reputation Health and well-being - amount of time spent online (internet or gaming). Sexting (sending and receiving of personally intimate images). Copyright (little care or consideration for intellectual property and ownership – such as music and film).

eSafety -Across the curriculum

It is vital that children are taught how to stay safe, protect themselves from harm and take a responsible approach to their own and others' eSafety.

Our school provides relevant, flexible and engaging eSafety education to all children as part of their curriculum entitlement and consider the following points:

- eSafety teaching within a range of curriculum areas is undertaken with each age group and is progressive throughout the school
- eSafety education is differentiated for children with special educational needs according to their specific needs/IEP
- We have an additional focus on safety during National safety Awareness week.
- Through letters to parents, children are made aware of the relevant legislation when using the Internet e.g. Data Protection Act (1998) and copyright implications
- Children are made aware of the impact of cyberbullying and how to seek help if they are affected by these issues through the taught curriculum
- Children are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions
- We ensure that children develop an understanding of the importance of the Acceptable Use Policy and are encouraged to adopt safe and responsible use of ICT both within and outside school
- Children are reminded of safe Internet use through e.g. classroom displays, eSafety rules (Appendices D & E), acceptance of site policies when logging onto the school network /Virtual Learning Environment

eSafety – Raising staff awareness

- There is a planned programme of formal eSafety training for all teaching and non-teaching staff to ensure they are regularly updated on their responsibilities as outlined in our school policy, and in September Inset on Working Safer Practice. Annual training register initially through LEA then SLT.
- All staff are expected to promote and model responsible use of ICT and digital resources. eSafety training is provided within an induction programme for all new staff to ensure that they fully understand both the school's eSafety Policy and Acceptable Use Policy
- regular updates on eSafety Policy, Acceptable Use Policy, curriculum resources and general eSafety issues are discussed in staff/team meetings.
  The impact of training is monitored through staff evaluations , half term reports in staff meetings and updates as deemed appropriate to e-safety issues.

eSafety – Raising parents/carers awareness

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it." (Byron Report, 2008).

Our school offer regular opportunities for parents/carers and the wider community to be informed about eSafety, including the benefits and risks of using various technologies both at home and at school. This is achieved through:

- School newsletters
- Homework diaries
- School website
- Parents eSafety Awareness sessions
- Promotion of external eSafety resources/online materials
- Parents to support e safety day
- School to provide information on the school notice board and displays

eSafety – Raising Governors' awareness

Governors, particularly those with specific responsibilities for eSafety, ICT or child protection, are kept up to date through discussion at Governor meetings and attendance at Local Authority Training.

NB: The eSafety Policy should be regularly reviewed and approved by the governing body.

Evaluating the impact of the eSafety Policy

It is important that we monitor and evaluate the impact of safeguarding procedures throughout school. This will be undertaken through:

- Questionnaires/ e-safety quizzes will be undertaken to establish if the eSafety policy is robust
- eSafety incidents are monitored, recorded and reviewed in the logbook
- SLT is responsible for monitoring, recording and reviewing incidents. The introduction of new technologies is risk assessed
- Incidents are analysed to see if there is a recurring pattern e.g. specific days, times, classes, groups and individual children
- These patterns will be addressed and the most effective procedure followed e.g. working with a specific group, class assemblies and reminders for parents
- The policy will be reviewed in accordance with incidents – legal advice will be sought if necessary
- Governors review the policy annually. The policy is published on the school website

Managing Filtering

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

Managing Videoconferencing & Webcam Use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher or teaching assistant before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with pupils is required.
- Personal mobile phones can only be used in staff areas, classroom when pupils are not present or when taken on school trips. A school mobile will be taken on out of school visits, and personal mobiles will be used by staff to reach other staff or for emergency calls.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Authorising Internet Access

- All staff must read and sign the Staff Code of Conduct and AUP policy before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Access to the Internet will be by directly supervised access to specific, approved on-line materials.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.

- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling E-safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.

- Any complaint about staff misuse must be referred to the Head Teacher. If the complaint is about the Head Teacher the referral must be made to the Chair of Governors.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- Discussions will be held with the Police Youth Crime Reduction to establish procedures for handling potentially illegal issues.

Community Use of the Internet

External organisations using the school's ICT facilities must adhere to the E- Safety policy.

USE OF MOBILE PHONES AND CAMERAS

This section is applicable to the whole of the school including Early Years Settings (3-5) under The Statutory Framework for EYFS requirements which came into force on 01.09.2012.

"The safeguarding policy and procedures must include an explanation of the action to be taken in the event of an allegation being made against a member of staff, and cover the use of mobile phones and cameras in the setting" EYFS 2012 s3.4.

In the event of an allegation, if against a member of staff then it will be taken to the head teacher. If it concerns the head teacher then it will be a matter for the Grievance and Discipline committee.

Children have their photographs taken to provide evidence of their achievements for developmental records (The Early Years Foundation Stage, EYFS 2012). Staff, visitors, volunteers and students are not permitted to use their own mobile phones to take or record any images of children for their own records during session times. Any photographs or filming must be done on schools equipment.

Procedures

- Under the Data Protection Act 1998, the school must seek parental consent to take photographs and use video recorders. Photographs will be stored on the school server. Once stored on the server they are deleted from the memory card.
- The schools digital camera/s or memory cards must not leave the school setting unless on an official school trip. Photos are printed and uploaded in the setting by staff and once done images are then immediately removed from the cameras memory.
- Staff, are the only ones to have access to photos. Once they have been finished with they are destroyed. Photographs containing images of looked after children will not be published on the website or in any school or external publication
- Parental Photography. We invite parents to take photos of their own children at the end of any event. All parents are reminded that photography and filming of children must not take place during events unless prior permission has been given, and must not be published on social network sites.
- Looked after children must not be photographed without consultation and permission of the social worker. The School will take appropriate action if necessary. All staff must work with the DSL when organising any events regarding a looked after child.

- Staff Mobiles. Most mobile phones have inbuilt cameras and internet access. The school policy allows staff to receive and make calls, but only in the confines of their empty classroom, staff room or office areas. Private mobiles must not be used in view of the children.
- If a situation arises where staff are expecting an urgent call, or they need to be contacted in an emergency, staff can leave their mobile phone in the office, and give permission for office staff to answer. Office staff will only inform caller to hold while they immediately go and inform staff member to come to the office to take the call. If staff has to make a private urgent call they may do so in the staff room or Heads office.
- All Cameras and mobile phones are prohibited in all toilet areas.