WHITEFIELD PRIMARY SCHOOL

HEALTHY HEARTS; HEALTHY BODIES; HEALTHY MINDS

Online Safety Policy

The Governing Board of *Whitefield Primary School* adopted this policy on 9th January 2019.

This policy will be reviewed on an annual basis by the Headteacher.

Signed by:

	Headteacher	Date:	
	Chair of governors	Date:	

Last updated: 9th January 2019

Contents

1. Aims

Our school aims to:

- *Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors*
- *Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology*
- *Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate*

'At Whitefield Primary school, we use technology when appropriate to enhance the learning experience for our children and to support the daily organisation and administration tasks carried out by school staff. Keeping members of our school community safe, whilst using technology, is a priority and we expect staff to act as role models in their use of technology and abide by the shared decisions reflected in our eSafety policy. Children are encouraged to explore and make responsible decisions regarding their uses of technology, informed by 'education' as opposed to the imposition of restrictions. As children are engaging with 21st Century technologies both inside and outside of school, we will provide opportunities for both children and the wider community to understand and view eSafety education as a key life skill. Our eSafety Policy defines what we consider to be acceptable and unacceptable behaviour regarding the uses of technology in school and the sanctions or procedures to be followed should breaches of security occur. It is communicated to staff, governors, pupils and parents and is updated in light of the introduction of new technologies or incidents.'

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governors has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governors will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is ??????????????

All governors will:

Ensure that they have read and understand this policy

Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

The DSL (Designated Safeguarding Lead) is Sarah Foster, Headteacher.

The Back Up DSL's are:

Janice Adams, Assistant Headteacher

Vicky King, Assistant Headteacher

Sarah Willers, Assistant Headteacher

Julie Garry, School Business Manager

Rebecca Caslake, Learning Mentor

The DSL takes lead responsibility for online safety in school, with support from the Back Up DSL's, in particular:

Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

Working with the headteacher, Comptuing Subject Leader, ICT Technician and other staff, as necessary, to address any online safety issues or incidents

Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)

Liaising with other agencies and/or external services if necessary

Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT managers (including Technician) – UPDATE THIS BIT – ASK CHRIS FOR WORDING

The ICT managers (subject leader, VIRTUE computers and Lancsngfl/CLEO) are responsible for:

Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

Conducting a full security check and monitoring the school's ICT systems on a weekly basis – Thursday PM

Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

Maintaining an understanding of this policy

Implementing this policy consistently

Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)

Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

Notify a member of staff or the headteacher of any concerns or queries regarding this policy

Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues

Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics

Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

All visitors will be presented with a summary e-safety document on arrival at the school office.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. At Whitefield Primary School, all children will complete a 'back to basics' e-safety unit of work annually (Autumn Term). This will be continued throughout the Year and built upon on a regular basis.

In **Key Stage 1**, pupils will be taught to:

Use technology safely and respectfully, keeping personal information private

Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

Use technology safely, respectfully and responsibly

Recognise acceptable and unacceptable behaviour

Identify a range of ways to report concerns about content and contact

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies throughout the year.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHCE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

Cause harm, and/or

Disrupt teaching, and/or

Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

Delete that material, or

Retain it as evidence (of a criminal offence or a breach of school discipline), and/or

Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school CHANGE IN LINE WITH NEW PROCEDURES

Pupils who walk to and from school without a parent or guardian may bring mobile phones into school. On entry to school at 8.50am, the pupil must bring their mobile phone to the main school office for storage during the day. They must collect their mobile phone at 3.30pm from the school office.

Year 6 pupils are allowed to bring their mobile phones or other devices in to school on their last day of term however access to these devices will be limited and monitored by the class teacher.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school – NO USB DEVICES

Staff members using a work device outside school must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices must not be used to save data relating to the school. Staff must use Google Drive to access their resources and school files and should not use USB devices.

If staff have any concerns over the security of their device, they must seek advice from the computing subject leader and/or the ICT technician.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. This will take the form of Hays Online Safeguarding Child Protection Level 3 training and 1:1 WRIST CPL1 training.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). This will take the form of Hays Online Safeguarding Child Protection Level 3 training and weekly LCC 7-minute briefings.

The DSL and Back Up DSL's will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online

safety at regular intervals, and at least annually. This will take the form of Hays Online Safeguarding Child Protection Level 3 training annually and LCC/Phil Threlfall DSL training every two years.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. . This will take the form of Hays Online Safeguarding Child Protection Level 3 training.

Volunteers will receive appropriate training and updates, if applicable.

All visitors will receive a summary e-safety document on arrival at school.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed yearly by the Subject Lead and Headteacher. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

Child protection and safeguarding policy

Behaviour policy

Staff disciplinary procedures

Data protection policy and privacy notices

Complaints procedure

GDPR Data Protection policy

Whistleblowing Policy

Social Media Code of Conduct for Parents

Staff Code of Conduct

14. Infrastructure and technology

Infrastructure and technology

Internet content filtering is provided by default as we subscribe to the Lancsngfl/CLEO

Broadband Service. It is important to note that the 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. School must ensure this is installed on computers in school and then configured to receive regular updates.

Further information can be found at www.lancsngfl.ac.uk/esafety.

Pupil Access:
Children should only access school ICT equipment and online materials when supervised by a trusted adult.

Passwords:

All users who have access to areas of the school network that contains sensitive data **must** have a secure username and password.

The administrator password for the school network is available to the Headteacher and Computing Subject Leader.

Staff and pupils should be regularly reminded of the importance of keeping passwords secure.

Passwords will be changed every six months.

Passwords should be a mixture of numbers and letters.

Software/hardware:

All software used by school should have the correct permissions and licenses for it to be used legally.

An up to date record of appropriate licenses will be kept by the school business manager.

Software will be evaluated in consultation with the ICT subject leader before it is installed on school systems. This includes iPads.

iPads will use 'Meraki' to install apps onto the iPads. This will be carried out by the ICT support or the Subject Leader. All requests must be sent to the Computing Subject Leader using the APP Request Form located on the school google drive. The APP must be agreed before they are installed on the iPads.

Managing the network and technical support:

Servers, wireless systems and cabling are securely located and physical access restricted.

- All wireless devices have their security enabled.
- Wireless routers are accessible only through a secure password.
- Access Area are responsible for managing the security of our school network, in
- consultation with the Headteacher and ICT subject leader.
- The safety and security of our school network is reviewed annually.
- Computers are regularly updated with critical software updates/patches.
- Users (staff, pupils, guests) have clearly defined access rights to the school network e.g. they have a username and password and permissions are assigned dependant on their position in the school.
- Staff and pupils are required to lock or log out of a school system that contains sensitive data when the computer/digital device is left unattended.
- Users should report any suspicion or evidence of a breach of security.
- Staff must use Google Drive as a replacement for USB devices.
- School equipment is for the use of school staff only and should not be used by other members of the staff's family. Devices used in school that are not school property should not contain personal data. (See Staff Code of Conduct and information below).
- Any network monitoring that takes place is in accordance with the Data Protection Act (1998).

Acceptable Use of Mobile Phones – staff and visitors
In our school the following statements outline what we consider to be acceptable and unacceptable use of mobile telephones:

- The school allows staff to bring in personal mobile telephones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a current pupil or parent/carer using their personal device.
- Staff and visitors should not use school internet on their personal mobile devices.

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- All staff must ensure that their mobile telephones/devices are left inside their bag throughout contact time with children. Staff bags should be placed in a stock cupboard or other suitable cupboard unless instructed by the Headteacher to move them to another appropriate location.
- With the consent of the Headteacher a member of staff may use a smart phone to support lessons.
- Mobile phone calls may only be taken at staff breaks or in staff members' own time and in the designated staff area.
- If staff have a personal emergency they are free to use the school's phone or make a personal call from their mobile in the designated staff areas, i.e. staffroom, PPA room, Acorn Meeting room.
- If any staff member has a family emergency or similar and required to keep their mobile phone to hand, prior permission must be sought from the Headteacher and the mobile phone be kept on silent mode in a pocket. The staff member must remove themselves from the vicinity of the children when the call is received.
- All volunteer helpers/students will be requested to place their bag containing their phone in an appropriate location and asked to take or receive any calls in the staffroom.
- Visiting contractors/professionals will be informed of the school's policy and asked to refrain from using mobile devices whilst in the school, or directed to the designated area.
- During group outings nominated staff will have access to the school's nominated mobile phone, which is to be used for emergency purposes only.
- It is the responsibility of all members of staff to be vigilant and report any concerns to the Headteacher.
- Concerns will be taken seriously, logged and investigated appropriately.
- The Headteacher or Deputy in her absence reserves the right to check the image contents of a member of staffs mobile phone should there be any cause for concern over the appropriate use of it.
- Should inappropriate material be found then the Local Authority Designated Officer (LADO) will be contacted immediately. We will follow the guidance of the LADO as to the appropriate measures for the staff member's dismissal.

15. Practices

Dealing with Incidents
Any breach of the Acceptable Use Policies will need to be dealt with in the appropriate way, depending on the incident and who has breached the AUP. An incident log is available via Google Drive and all incidents must be reported here. This must be brought to the attention of the DSL or Back Up DSL immediately. This must be audited on a regular basis by the Subject Leader, the Headteacher and the Computing Governor. This is accessible via 'Google Drive' and is stored online.

Illegal offences
Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher 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. 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 school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with 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 • 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 DSL • Enter the details in the Incident Log • Additional awareness raising of eSafety issues and the AUP with individual classes/child • More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy • Consider parent/carer involvement
Deliberately searching for inappropriate materials	
Bringing inappropriate electronic files from home	
Using chats and forums in an inappropriate way	

Appendix 1: acceptable use agreement (pupils and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers	
Name of pupil:	
When using the school's ICT systems and accessing the internet in school, I will not: *Use them for a non-educational purpose* *Use them without a teacher being present, or without a teacher's permission* *Access any inappropriate websites* *Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)* *Use chat rooms* *Open any attachments in emails, or follow any links in emails, without first checking with a teacher* *Use any inappropriate language when communicating online, including in emails* *Share my password with others or log in to the school's network using someone else's details* *Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer* *Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision* If I bring a personal mobile phone or other personal electronic device into school: *I will take it to the school office at 8.50am for storage during school hours and pick it up at 3.30pm* I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's ICT systems and internet responsibly.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not: *Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature* *Use them in any way which could harm the school's reputation* *Access social networking sites or chat rooms* *Use any improper language when communicating online, including in emails or other messaging services* *Install any unauthorised software* *Share my password with others or log in to the school's network using someone else's details*	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**