The Westminster School

E-Safety Policy inc Internet Access and Acceptable Use Policy 2017/2018

Safe Happy and Learning Together

Building foundations and providing opportunities to create confident, aspirational and independent members of our community.

Approved by Governing Body on:	08/06/18
Signed by Chair of Governors:	Ken Ohs
Head Teacher:	C A Hill BEd NPQH
Lead Personnel:	O Flowers
Date of Review:	08/06/19

Rationale

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the real world. Increasingly, children are accessing material through the internet and games consoles which is not age appropriate. It is essential to address this and to encourage a lifestyle which incorporates a healthy balance of time spent using technology.

This policy, supported by the Acceptable Use Policies (AUP; see appendices) for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies: Child Protection, Bring Your Own Device (BYOD), Health and Safety, Behaviour and SHaLT.

Both this policy and the Acceptable Use Policies (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet, technologies provided by the school (such as PCs, laptops, whiteboards, tablet, voting systems, digital video and camera equipment, etc) and technologies owned by pupils or staff.

The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging
- Blogs
- Social networking sites
- Chat Rooms
- Gaming Sites
- Text messaging and picture messaging
- Video calls
- Podcasting
- Online communities via games consoles
- Mobile internet devices such as Smart Phone and Tablets.

Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

1. An effective range of technological tools which are filtered and monitored;
2. Policies and procedures, with clear roles and responsibilities;

3. A comprehensive e-Safety education programme for pupils, staff and parents.

Staff Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head Teacher, with the support of governors, aims to embed safe practices into the culture of the school. The Head Teacher ensures that the policy is implemented and compliance with the policy monitored. All staff are encouraged to create a talking culture in order to address any e-safety issues which may arise in classrooms on a daily basis. All visitors also receive our e-safety agreement on arrival at school.
The responsibility for e-Safety has been designated to a member of the senior leadership team.

Our school **e-Safety Coordinators** are **Oliver Flowers** and **Jonathan Billington**.

Our e-Safety Coordinators ensures they keep up to date with e-Safety issues and guidance through liaison with Broadband Sandwell's e-Safety Officer and through organisations such as The Child Exploitation and Online Protection (CEOP) and 360 degree safe. The school's e-Safety Coordinators ensures the Head, Senior Management and Governors are updated as necessary.

Staff awareness

- All staff receive regular information and training on e-safety issues in the form of in house training and meeting time.
- New staff receive information on the school's AUP as part of their induction.
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas and through a culture of talking about issues as they arise.
- E-safety records of concern are completed by staff as soon as incidents occur and are reported directly to the school's designated safeguarding team, Mrs Joanne Turner, Ms Charlotte Stubbs, Miss Penny Cartwright.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. These behaviours are summarised in the AUPs which must be signed and returned before use of technologies in school.

Internet:

- The Westminster School will use TrustNet "filtered" Internet Service, which will minimise the chances of pupils encountering undesirable material.
- Staff, pupils and visitors have access to the internet through the school's fixed and mobile internet technology.
- Staff should email school-related information using their Openhive/@westminster.sandwell.sch.uk address and not personal accounts.
- Staff will preview any websites before recommending to pupils.
- Internet searches are conducted using the Safe Search homepage found at http://www.safesearchkids.com/.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.
- The CEOP Report Abuse button is available on the school website and the school landing page.
- Teachers make children aware of this and when it is appropriate to use it.
- The Bully Watch button is available on the school website taking them to http://www.bully-watch.co.uk/ (more specifically http://www.bully-watch.co.uk/sl/?schoolName=WSTMNS#) and Teachers make children aware of this and when it is appropriate to use it.
- If staff or pupils discover an unsuitable site, the screen must be switched off immediately and the incident reported to the e-safety coordinator(s) detailing the device and username. Agilisys can then be informed and contact to TrustNet can be instigated.
- Staff and pupils are aware that school based email and internet activity is monitored and can be explored further if required.
- Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher and then Agilisys so that the Service Provider (TrustNet/Virgin Media) can block further access to the site.
- Pupils are expected not to use any rude or offensive language in their email communications and contact only people they know or those the teacher has approved.
- They are taught the rules of etiquette in email and are expected to follow them.
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.
- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be sanctioned following the school's behaviour policy.
- A summary of these ICT rules are displayed in the ICT suite and all areas with ICT resources. Pupils will be asked to sign to this agreement, ensuring that they are aware of expectations. (See Appendix). Copies of the agreement will also be distributed to parents to ensure that key messages are reinforced at home.

- The internet use agreement also appears when children log in to networked computers in school. They are required to click to agree to the policy before they are allowed to use the computers.

Passwords:

- Use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers).
- Passwords should not be written down.
- Passwords should not be shared with other children or staff.

Mobile technology (laptops, iPads, netbooks, etc):

- Staff laptops should not be left in cars. If this is unavoidable, it should be temporarily locked out of sight in the boot.
- Staff should only use the laptop which is allocated to them.
- Mobile technology for pupil use, such as Nexus 7s, iPads and netbooks, are stored in a locked cupboard. Access is available via the school office keyholders or Agilisys. Members of school staff (not visitors or children) should sign in/out the technologies before and after each use.
- Mobile Technology assigned to a member of staff as part of their role and responsibility must have a passcode or device lock so unauthorised people cannot access the content.
- When they are not using a device staff should ensure that it is locked to prevent unauthorised access.
- No personal devices belonging to staff or children are to be used during lessons at school unless covered by the Bring Your Own Device Policy. If staff bring in their own devices such as mobile phones, these are to be used during break times only and kept on silent. If pupils bring in mobile phones (for the purpose of safety if they walk to and from school alone), they should be kept switched off and out of sight all day, and will remain the responsibility of the child in case of loss or damage. Any children not following these rules will be dealt with using the school's behaviour policy.

Data storage

- Staff are expected to save all data relating to their work to their Laptop if they have been assigned one or to the Google Drive Account.
- The school discourages the use of removable media however if they are used we expect the Encryption of all removable media (USB pen drives, CDs, portable drives) taken outside school or sent by post or courier.
- Staff laptops should be encrypted if any data or passwords are stored on them.
- IEPs, assessment records, pupil medical information and any other data related to pupils or staff should not be stored on personal memory sticks but stored on an encrypted USB memory stick provided by school or on our secure SharePoint platform.
- All staff are required to sign a personal data encryption agreement before being issued with an encrypted memory stick. (See appendix).
- Only take offsite information you are authorised to and only when it is necessary and required in order to fulfil your role. If you are unsure speak to a member of the Senior Management Team.

Social Networking Sites

- Use such sites with extreme caution, being aware of the nature of what you are publishing on-line in relation to your professional position. Do not publish any information online which you would not want your employer to see.
- Under no circumstances should school pupils or parents, past or present, be added as friends, unless known to you as a friend or relative prior to your appointment.
- Your role in school requires a high degree of professionalism and confidentiality.
- Any communications or content you publish that causes damage to the School, Local Authority, any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the School and Local Authority Dismissal and Disciplinary Policies apply.
- Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct.
- The Local Authority expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

Any communications made in a professional capacity through social media must not either knowingly or recklessly:

- place a child or young person at risk of harm;
- bring the School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting images that are discriminatory or offensive or links to such content.

The School reserves the right to monitor staff internet usage. The School considers that valid reasons for checking internet usage include concerns that social media/internet sites have been accessed in breach of this Policy.

Digital images

- Use only digital cameras and video cameras provided by the school and under no circumstances use personal equipment such as digital cameras or camera phones to store images of children unless prior authorisation has been provided with the BOYD policy. If it is used in this way then images must be removed before leaving the school premises.
- Ensure you are aware of the children whose parents/guardians have **not** given permission for their child's image to be used in school. An up to date list is kept in the school administrative office.

- When using children's images for any school activity, they should not be identified by their name.

Members of staff who breach the acceptable use policy may face disciplinary action. A misuse or breach of this policy could also result in criminal or civil actions being brought against you.

Providing a comprehensive E-safety education to pupils and parents

- All staff working with children must share a collective responsibility to provide e-safety education to pupils and to promote e-safety in their own actions.
- Formally, an e-safety education is provided by the objectives contained in the ICT unit plans for every area of work for each year group. Even if e-safety is not relevant to the area of ICT being taught, it is important to have this as a 'constant' in the ICT curriculum.
- Informally, a talking culture is encouraged in classrooms which allows e-safety issues to be addressed as and when they arise.
- The ICT Coordinator will lead an assembly twice a year, including on Safer Internet Day, highlighting relevant e-safety issues and promoting safe use of technologies.
- All classes will follow a themed week at least once per year, during which their class teacher will lead lessons and activities designed to educate children in keeping safe when using the internet and other new technologies.
- eSafety themes are also woven into the fabric of the school curriculum through SHaLT.
- Staff will ensure children know to report abuse using the CEOP button widely available on many websites or to speak to any member of staff, who will escalate the concern to the ICT Coordinator with responsibility for E-safety.
- When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's ICT guidelines. (See Appendix)
- Parents/carers will be invited to attend an e-safety awareness workshop once per year, run by the school staff.
- Children will have the opportunity to educate parents through assemblies and classroom activities on an annual basis.

Maintaining the security of the school IT Network

Agilisys maintains the security of the school network and is responsible for ensuring that virus protection is up to date at all times. However, it is also the responsibility of the IT users to uphold the security and integrity of the network.

Virtual Learning Gateway (VLE)

Staff and pupils have access to the SharePoint, provided and maintained by Agilisys.

Pupils/staff details or sensitive, confidential information will be stored on here and all login credentials including passwords must not be written down.

All classes may provide work for publication on SharePoint and digital images and work can be stored. Subject staff will be responsible for ensuring that the content of the pupils' work is accurate and the quality of presentation is maintained. All material must be the author's own work, crediting other work included and stating clearly that author's identity and/or status.

Complaints procedure

As with other areas of school, if a member of staff, a child or a parent / carer has a complaint or concern relating to e-safety then they will be considered and prompt action will be taken. Complaints should be addressed to the e-safety Coordinator in the first instance, who will undertake an immediate investigation and liaise with the leadership team and those members directly involved. Incidents of e-safety concern will be recorded using a Record of Concern proforma and reported to the school's designated safeguarding officer in accordance with school's child protection policy. Complaints of Cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

Monitoring

The Head Teacher/Deputy Head Teacher or other authorised members of staff may inspect or monitor any ICT equipment owned or leased by the school at any time without prior notice.

Monitoring includes: intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, e-mail, texts or image) involving employees without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures, to ensure the effective operation of School ICT, for quality control or training purposes, to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

Breaches of Policy

Any policy breaches are grounds for disciplinary action in accordance with the School Disciplinary Policy. Policy breaches may also lead to criminal or civil proceedings.

Incident Report

All security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Designated Safeguarding Person either Christine Hill, Joanne Turner, Charlotte Stubbs or one of the e-Safety coordinators Oliver Flowers or Jonathan Billington.

The Westminster School
ICT Acceptable use policy for pupils for use at home (H) and at school (S).

The school has installed computers and Internet access to help our learning. These rules will keep us safe and help us to be fair to others.

- I will only use ICT in school for school purposes. (S)
- I will ask permission from a member of staff before using the Internet and will only be online when an adult is in the room. (S)
- I will only use my login and password and never share these with others. (S) (H)
- I will ask permission before bringing in memory sticks or CD ROMs into school. (S)
- I will only open and delete my own files. (S)
- The messages I send will be polite and sensible. (S) (H)
- I will never give out my own or other people's name, address or phone number online. (S) (H)
- I will never upload any images of school activities to any social networking site. (S) (H)
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. (S) (H)
- If I see anything I am unhappy with on the computers, I will turn the screen off and tell my teacher or an appropriate adult straight away. (S) (H)
- I understand that the school can check my computer use and that my parents/carers can be contacted if school staff are concerned about my e-safety. (S)

Pupil Signed: _____ Date:_____

Parent Signed: _____ Date:_____

The Westminster School
ICT Acceptable use policy for staff, governors and visitors

These rules are designed to protect staff and visitors from e-safety incidents and promote a safe e-learning environment for pupils.

- I will only use the school's internet, email, computers, laptops and mobile technologies for professional purposes as required by my role in school.
- I will not disclose my password to anybody else.
- When accessing school email, SharePoint or any other sensitive information relating to The Westminster School, employees will ensure that it is conducted on a device that had the appropriate security measures (anti-virus, firewall, encryption) and that locked out when away from the device and logged off each of the sites after use.
- I will ensure that any online communications with staff, parents and pupils are compatible with my professional role.
- I will not give out my own personal details to pupils or parents.
- I will send school business emails using my school email address, if I have been provided with one, not my personal email address.
- I will ensure any data that I store is stored on a secure, encrypted device.
- I will not browse, download, upload or distribute any material which could be considered offensive, illegal or discriminatory.
- Images of pupils will only be taken and used for professional purposes in line with school policy with consent of the parent or carer. Images will not be distributed outside of school without the permission of the parent/carer and Head Teacher.
- If it is necessary to bring my own personal devices into school, these will only be used during non-contact time without pupils.
- **I will report any e-safety concerns to the designated safeguarding officer immediately using the E-safety Record of Concern.**
- **Mobile phones will be out of sight and switched to silent.**
- **I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.**
- **I will support the school's e-safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.**

I understand the procedures and agree to follow them with immediate effect.

Print Name: _____

Signed: _____ Date: _____

The Westminster School
Data Security

Following a review of procedures in place to store sensitive data in line with National recommendations the following practice is to be adhered to:-

> ***Sensitive data consists of any information which is personal to individuals or deemed sensitive or valuable to the school.***

Staff should only save sensitive data in the following secure formats:-

1. On the learning platform (SharePoint)
2. On the encrypted USB memory stick provided
3. On the encrypted laptop provided
4. Onto the Google Drive account provided as part of your employment (@westminstercloud.co.uk)

This ensures that no legal action can be taken for lost data.

Staff are encouraged to hold all of their data on their school laptop that has a built-in level of encryption. If this is not possible and they have not been allocated a laptop they are encouraged to save all of the data onto their Google Drive account provided as part of their employment. The password for this account should not be written down anywhere and the Google Drive Account should be logged out or lock when not in use.

If you lose your encrypted memory stick or are unable to open it because of a password error, you must inform the Deputy Head Teacher(s) or Head Teacher without delay. It is imperative that you do not share or write down your password. You may add a question prompt reminder when first accessing your memory stick, which can be used if you have forgotten your password. It is your responsibility to keep the data from your memory stick regularly backed up in another secure format as detailed above. Sensitive data should not be sent via email to external agencies, third party agencies or those no employed by the school unless it is encrypted/password protected.

Failure to follow these guidelines will be treated seriously and could lead to disciplinary procedure.

I understand the procedures and agree to follow them with immediate effect.

Name _____ Signed_____

Date _____

E-Safety Record of Concern

<table>
<tr><td>Name of Child</td><td colspan="3"></td></tr>
<tr><td>DOB</td><td colspan="3"></td></tr>
<tr><td>Date of incident/disclosure</td><td></td><td>Time</td><td></td></tr>
<tr><td>Names of any other Staff/Children Present</td><td colspan="3"></td></tr>
<tr><td rowspan="2">Record any disclosure from the child using their words. Use:
• Tell
• Explain
• Describe
• Outline

To clarify/gather information
USE NO FURTHER QUESTIONS.</td><td colspan="2">Who?</td><td>What?</td></tr>
<tr><td colspan="2">Where?</td><td>When?</td></tr>
<tr><td>Why are you concerned about the child?</td><td colspan="3"></td></tr>
<tr><td>Detail anything you have observed and when.</td><td colspan="3"></td></tr>
<tr><td>Detail any websites/games/films the child discussed with</td><td colspan="3"></td></tr>
</table>

you. Please include Avatar names, online friends names where known.			
What catergory does the disclosure best fit with?	Grooming		
	Cyberbullying		
	Misuse of Social Networking site		
	Sexting		
	Gaming		
	Underage Films		
	Misuse of Digital Camera		
	Other (please specify)		
Detail anything you have heard and when.			
Detail anything you have been told, by who and when.			
Name (Print)		Date	
Position:		Signature	

E-Safety Record of Action

Name of e-Safety Coordinator/DSP record of concern handed to:	
Date:	
Action(s) to be taken:	
Outcomes of action:	
Name (print):	Date:
Designation:	Signature: