Ash Villa School

E-SAFETY AND ACCEPTABLE USE POLICY

E-SAFETY and ACCEPTABLE USE POLICY

Policy Review Date and Contact

This policy is due for review:	Autumn Term 2016-17
Member of staff responsible for policy:	Leigh Bentley

Approved by the school's Governing Body:

(Signed) _____ Chair of Governors

(Signed) _____ Headteacher

This e-safety policy has been created using guidance published by Lincolnshire County Council (LCC), Lincolnshire Safeguarding Children Board (LSCB) and the DfE: *Keeping Children Safe in Education (2016) Annex C Online Safety*. The policy also details the acceptable use of ICT equipment and resources at Ash Villa School for all staff and students. The policy is reviewed annually.

All students (see Appendix 1) and staff (see Appendix 3) will be made aware of its content and are asked to sign a checklist agreeing to adhere to the policy when using the equipment and resources Agreements are in student's planners, which are explained to the student, discussed as required and signed as part of the admission process to school.

E-safety Officer

The school's designated e-safety officer is the school's designated safeguarding officer.

The facts about being online

87% of children go online at home, 51% of teenagers have revealed information online that could be used to identify them, 29% of friends children aged 12 to 15 have online are not personally known to them. These are just a few of the facts that Ofcom have found in their Children and Parents: Media Use and attitudes Report (Oct 2014 and 2013).

Keeping children safe online is a daunting task and it is important to understand the variety of things children can come across:

- Inappropriate content
- Cyberbullying
- Online grooming
- Sexting
- Online reputation
- Privacy and identity theft
- Online pornography

What technology are children using?

There are a variety of ways children use technology, including:

- Social networking
- Online gaming
- Apps
- Mobile phones
- Tablets
- Chatting using chatrooms, skype, instant messaging

Learning more about these activities and getting advice on how to manage this is a positive step to keeping children safe online.

E-Safety is used to describe pro-active and reactive measures of educating and safeguarding children and young people, and adults working with them, while they use digital technology. In order for children and young people to remain safe, they should be educated not only in the dangers but also informed about who they can contact should they feel at risk and where to go for advice while still promoting the many benefits of using digital technology.

- E-Safety concerns safeguarding children and young people in the digital world.
- E-Safety emphasises learning to understand the use of technologies in a positive way.
- E-safety is less about restriction and more about the education about the risks as well as the benefits, so users can feel confident online.
- E-Safety is concerned with supporting children and young people to develop safer online behaviours in and out of school.

The objective of this policy is to describe the procedures and systems in place to ensure staff and pupils remain safe when using digital technology at Ash Villa School.

Responsibilities of the School and Staff

All staff should sign the AUP (see Appendix 3) on appointment and after every review of the policy. Staff thereby accept that the school can monitor network and Internet usage to help ensure staff safety.

All staff are provided with email accounts for use of official school business.

School staff are able to confiscate student's mobile phones and any electronic device, when students have brought these into school, without previously gaining consent from the Head teacher. It is the stated policy of Ash Villa School that mobile phones should not be accessed by students in school nor should any electronic device that has internet or camera capabilities . Staff should follow DfE publication *Searching, screening and confiscation Advice for headteachers, school staff and governing bodies* February 2014 when doing so. Any item confiscated in school will be handed over to the inpatient team for returning to parent/carers.

E-Safety and School Staff

The following is the minimum requirements to which all school staff should adhere to, as per guidance from LSCB:

Internet access – staff must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues.

It is recognised that under certain circumstances inadvertent access may happen. For example, a school researching the holocaust may produce results with Nazi propaganda. Should you or a student access any of these sites unintentionally you should report the matter to the Headteacher so that it can be logged. Access to any of the following should be reported to Lincolnshire Police: images of child abuse (sometimes incorrectly referred to as child pornography).These are images of children apparently under 16 years old involved in sexual activity or posed to be sexually provocative; adult material that potentially breaches the Obscene Publications Act; and criminally racist material in the UK.

Social networking – is not allowed in our school. Staff receive education in the dangers of Social Networking sites and guidance in their use. Staff should fully acquaint themselves with the privacy settings that are available on any social networking profile in order that profiles are not publicly available. Members of school staff should never knowingly become 'friends' with current or former pupils on any social networking site or engage with pupils on internet chat.

Use of Email - All members of staff should use their professional email address for conducting school business. Use of school email for personal/social use is permitted, but care should always be taken never to do or say anything that might reflect on the reputation of Ash Villa School.

Passwords - Passwords are confidential and individualised to each person. On no account should a member of staff allow a student to use a staff login.

Data Protection - Where a member of staff has to take home sensitive or confidential information sufficient safeguards should be in place to prevent loss or misuse, i.e. is it really necessary to take it all home, can it be encrypted, does it have to be on a USB memory stick which can be easily misplaced.

File sharing - technology such as peer to peer (P2P) and bit torrents are not permitted on the Lincolnshire School's Network.

Personal Use - Staff are permitted to use ICT equipment for personal use. The school emphasises that all use should be within the boundaries of acceptance.

Images and Videos - Staff should not upload onto any internet site, images or videos of other staff or pupils without consent nor of themselves on school business without the consent of the Headteacher.

Use of Personal ICT - use of personal ICT equipment is permitted at school e.g. a USB pen stick. Any such use **MUST** be stringently checked with up to date anti-virus and malware checkers. The school is not responsible for any loss / damage to personal equipment used in school.

Viruses and other malware - any virus outbreaks are to be reported by the member of staff affected or member of staff in charge of the student/class affected to the Kier Helpdesk as soon as it is practical to do so, along with the name of the virus (if known).

Internet filters and monitoring - As a Lincolnshire County Council school Ash Villa School's IT system uses a web filter with the aim of screening inappropriate websites and content. In addition Ash Villa School uses Future Digital Forensic Software to monitor staff and student activity and to enable response to inappropriate internet use and/or inappropriate use of IT resources.

Use of Mobile Phones by Staff, Governors and Visitors

All staff, governors and visitors should ensure that personal mobile phones are switched to silent in school during periods of the day when students are present. In addition teaching staff should ensure mobile phones are switched off when teaching students. An exception to this is when school staff are off school premises with students as mobile phones may need to be used immediately in case of emergency.

Staff Awareness of Acceptable Use

All staff are provided with a copy of this policy upon appointment and following each review and sign an agreement to abide by its contents (see Appendix 3). Copies of signed staff agreements are kept in the member of staff's personal file.

E-Safety and Students

Images and Videos - pupils should not upload onto any internet site, images or videos staff or other pupils without consent.

Use of the Internet – pupils at Ash Villa School have access to the internet to assist in research and online activities related to their education.

Logins, Passwords and User Areas – pupils at Ash Villa School are allocated an individual login with password and user area to store all electronic work. Pupils sign an agreement to only access their user area. Staff can access their work and user areas at any point.

Social Networking – access to social networking sites is not permitted at Ash Villa School.

Email – pupils have access to electronic communication via their mainstream school website portals and the Ash Villa School email facility. Pupils are not permitted to access 'personal' email systems such as Hotmail.

Mobile Phones – pupils are not permitted to bring mobile phones into Ash Villa School or on educational visits, unless in exceptional circumstances agreed with the Head teacher.

All students should sign an Acceptable Use Policy (See Appendix 1) upon admission. Pupils accept thereby, that the school can monitor network and internet usage to help ensure pupil safety.

Photographs - Photographs taken of students should maintain their anonymity. Anyone taking photographs of students should refer to the consent forms signed by parents/carers in the school induction pack before taking photographs of students.

Students downloading photographs to their secure areas for further work, for example Photoshop editing, can only download images of objects and themselves. They cannot download images of other students. For further information please refer to the Safe Use of Children's Photographs Policy.

Students can access a variety of help, should they require it:

Child Line	0800 1111
Lincolnshire Safeguarding Children Board	01522 782111
Local Police	101
Emergency Police	999
CEOP	https://www.ceop.police.uk/
Staff at a school	
Unit Staff	
Parents/Carers/Responsible Adults	

Breaches of Acceptable Use

All breaches of acceptable use of IT equipment, both of students and staff, are recorded and dealt with in line with relevant school rules and disciplinary procedures. See Appendix 2 for a copy of the sheet used to record these events. The record sheets are retained by the school's DSO. See Appendix 4 for Incident Flowchart

All breaches of acceptable use should be reported to the Headteacher, at the earliest opportunity for appropriate action to take place.

Further actions may be required, depending on the seriousness of the incident, therefore the following options are available:

- Call the Customer Service Centre (CSC) of the Lincolnshire Safeguarding Children Board (LSCB) on 01522 782111
- Call the local police 101
- If there is immediate danger call the Police on 999

Staff and Student Awareness and Training

The school provides an annual safeguarding update for all staff, provided by LCC and delivered by the school's DSO. In addition the LCSB e-safety e-module is completed by all teaching staff. The DSO also completes additional training relating to e-safety. Please refer to a copy of the school's 5-year CPD programme for further details.

E-Safety is planned into the curriculum primarily through PSHE and computing. E-Safety workshops are also offered to students as part of an annual themed week relating to various aspects Personal Safety.

Appendix 1

Student Acceptable Use Policy

I agree to follow the expectations listed below when using ICT equipment and resources at Ash Villa School:

- I will not access **social networking sites**. If I am aware that such sites can be accessed I will inform a member of staff.
- I will only access my **own user** area and I will **not share my username/passwords**.
- I agree **school staff may review files** on my user area and monitor my use of the Internet and other IT resources to ensure that I am using the system responsibly.
- I will only use **memory sticks provided by Ash Villa School** unless Mr. Bentley has agreed for me to use my own or those provided by my mainstream school.
- I will **not bring my mobile phone** into school or on school visits. Nor will I bring my **ipod/electronic device** or anything that plays music, records, takes pictures or takes/receives phone calls, texts or emails
- I will only access **email through my mainstream school website**. I will not access email sites such as **Hotmail** and/or MSN. If I am aware that such sites can be accessed, I will inform a member of staff.
- I will return **digital cameras** and Nintendo DS equipment and games to the teacher who issued them at the end of each session.
- When downloading photographs I will only download photographs of myself and objects, **I will not download photographs of other students**.
- I will only take **photographs of the backs** of other students.
- I understand that Ash Villa School is **monitored by CCTV**.

Signed:_____ Date:_____

Appendix 2

Record of breaches of acceptable use of IT equipment and procedures.

What breach has occurred?
When did the breach occur? Date and Time
Who was involved?
Headteacher Informed Yes/No
E-Safety Officer Informed Yes/No
Details of action taken:
Breach Reported By (sign and print name):
Action Taken By (sign and print name):

Appendix 3

Ash Villa Acceptable Use Policy Staff Agreement

For **ALL** Ash Villa Staff to read the policy and sign.

I have been provided with access to the Acceptable Use Policy for IT equipment and procedures at Ash Villa School and agree to abide by its contents.

Signed	
Name	
Date	

Incident Flowchart

Appendix 4