ASHDOWN HOUSE E-SAFETY POLICY (to include boarding and day pupils)

eSafety Policy

Creating a Safe ICT Infrastructure in School

All users of the school's computer network have clearly defined access rights, enforced using a username/password login system. Account privileges are achieved through the file/folder permissions, and are based upon each user's particular requirements – children have much more limitations in place than individual staff members do with their personal logins, for example. This helps to protect the network from accidental or malicious attempts to threaten the security of it or the data accessible using it.

A permanently-enabled filtering system is provided, which is designed to filter out material found to be inappropriate for use in the education environment. At Ashdown we use **Baracuda**. As an additional safety measure, each individual web page is also dynamically scanned for inappropriate content as it is requested, categorised by its content and then access prevented to it if necessary.

Security software is installed on all *Windows* machines to prevent any malware (e.g. virus) attacks.

Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Professional conduct is essential. It is the responsibility of the user to ensure that they have logged off the system when they have completed their task and to keep their user credentials confidential to halt impersonation on the network.

Rules for Publishing Material Online (inc. Images of Pupils)

Whilst we wish the school's website to be a valuable tool for sharing information and promoting children's achievements with a global audience, we do recognise the potential for abuse that material published may attract, no matter how small this risk may be. Therefore, when considering material for publication on the website, the following principles should be borne in mind, in accordance with the GDPR and the school's *Safeguarding Policy*:

- If an image/audio/video recording of a child is used then they should not be named (including in credits) and ideally children should not be on their own.
- Pictures or recordings which are deemed to be of interest only to parents will be uploaded to the Parents Section of the website, which is password protected.
- Files should be appropriately named in accordance with these principles and care should be taken to include only suitable ALT tags as well.
- Only images of children in suitable dress should be used and group photographs are preferred in preference to individual photographs.
- Parents are given the opportunity to withdraw permission for the school to publish images/audio/video of their child on the school website.
- Content should not infringe the intellectual property rights of others – copyright may apply to: text, images, music or video that originate from other sources. All copied or embedded content should be properly referenced.
- Content should be polite and respect others. No image should embarrass, humiliate or belittle a child. Staff must be aware that images used could lead to peer on peer

abuse. Please refer to the *Safeguarding Policy*.

- Material should be proof-read (e.g. to check for spelling or grammatical errors) before being published.

Children will likely use a variety of online tools for educational purposes during their time at the school. Work produced in this way will be posted with a suitable level of anonymity.

Pupils' Rules for Acceptable Internet Use

Educational use of the Internet is characterised by activities that provide children with appropriate learning experiences. Clear rules which help children develop a responsible attitude to the use of the Internet have been devised. Clear expectations and rules regarding use of the Internet will be explained to all classes. A simplified version is also displayed within school to ensure that everybody is made aware of them.

- I will only use the internet when supervised or given permission from a member of staff to do the specific task
- I will not deliberately seek out inappropriate websites.
- I will report any unpleasant material to a member of staff immediately because this will help protect other pupils and myself.
- I will not download/install program files.
- I will ask permission before completing and sending forms/emails.
- I will be polite and respect others when communicating over the Internet.
- I will not give out any personal information over the Internet.
- I will not share my login details for websites with others.
- I understand that the school may check my computer files and monitor the Internet sites I visit.
- I will not use any personal devices in school which can access 3G or 4G
- I understand that I may not use certain social media sites such as *Facebook* which carry an age restriction (13 years old)
- Inappropriate use of social media sites (even in the holidays) may lead to disciplinary action according to Ashdown House's *Anti-bullying Policy* and *Promoting Good Behaviour Policy*

Children are encouraged to choose strong passwords to ensure no unauthorised people gain access to any of their accounts.

All children are given an account on the *Edmodo* virtual learning environment. This provides them with a secure area in which they: can communicate with others in their class, do homework tasks and access lesson resources.

Staff Rules for Acceptable Internet/Network Use

Users shall not visit internet sites, make, e-mail, post download, upload, data transfer, communicate, or pass on material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images (illegal – *The Protection of Children Act 1999*)
- Grooming, incitement, arrangements or facilitation of sexual acts against children (illegal – *Sexual Offences Act 2003*)
- Possession of extreme pornographic images (illegal – *Criminal Justice and Immigration Act 2008*)
- Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (Illegal – *Public Order Act 1986*)
- Pornography
- Illegal drugs
- Gambling
- Terrorism
- Radicalisation (for further guidelines, please refer to the *Safeguarding Policy*)
- Promotion of any kind of discrimination
- Promotion of racial or religious hatred
- Threatening behaviour, including promotion of physical violence or mental harm
- Any other information which may be offensive to colleagues or breaches the integrity of the school or brings the school into disrepute
- copy or modify copyright protected material downloaded from the Internet without authorisation.
- subscribe to a non-job related bulletin board, newsgroup or any other similar Internet service without obtaining the Head or Bursar's permission.
- enter into a contract via the Internet without following the School's standard authorisation procedures. A contract entered into via the Internet is likely to be legally binding in the same way as any other contract.
- use the Internet for criminal activity, for example but not limited to software and music piracy, terrorism or the sale of illegal drugs.

E-mail

Users should:

- adopt a responsible approach to the content of e-mails, bearing in mind that e-mails often need to be as formal as any other form of written correspondence such as a letter.
- be aware that e-mails are disclosable in any legal action against the School and e-mails which have been deleted by a user or from the network may be recovered.
- remember that e-mail correspondence is not private as e-mails can be easily copied, forwarded or archived without the original sender's knowledge. When drafting any e-mail a user should bear in mind that it may be read by a person other than the designated recipient.

Users should not:

- send an e-mail message which is abusive, malicious, discriminatory, defamatory about any person or organisation, or which contains illegal or offensive material or foul language.
- receive such an e-mail message and not inform the Head.

- send confidential information externally without express authority from the Head
- send information externally which may infringe the intellectual property rights of a person or organisation.
- fail to keep hard copies of e-mails where this is necessary for School records.
- send an e-mail from which the automatic School disclaimer has been deactivated or removed.
- open attachments to e-mails from unknown sources without obtaining the Head's permission.
- enter into a contract via e-mail without following the School's standard authorisation procedures. A contract entered into by e-mail is likely to be legally binding in the same way as any other contract.
- send unsolicited bulk e-mail messages or "spam".

Social Networking:

Communication with students (Including the use of technology)

Communication between pupils and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones, text messaging, e-mails, digital cameras, videos, web-cams, websites, social networking sites, online gaming and blogs – staff should not communicate with pupils other than through official school channels (school email address etc.) Adults should not share any personal information with a pupil. They should not request, or respond to, any personal information from the student, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny

Adults should also be circumspect in their communications with pupils so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers. E-mail or text communications between an adult and a pupil outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites, such as social networking, instant messaging or gaming.

Communication with ex-pupils is not advised. Please be aware that ex-pupils may be in contact with pupils who are still at the school.

Actions which bring the school into disrepute could lead to disciplinary procedures.

This means that staff should:

- not use internet or web-based communication channels to send personal messages to a student
- not to have images of students stored on personal cameras, devices or home computers.

- not make images of students available on the internet, other than through the school network/website, without permission from parents and senior teachers.
- Be cautious in their contact with ex-pupils, as there is still a professional relationship and there may be contact with current pupils.

Private use of social media

Private use of social media around the pupils is not accepted. The use of social media is permissible if it is for educational purposes with permission from the headmaster.

Staff must be considerate of their colleagues' reputation and be aware that private photos posted on social media could be seen by pupils and may even constitute abuse. Ashdown House is primarily a boarding school with many staff living on site and occasional social situations are acceptable in the privacy of one's own home (in line with the Occupancy Agreement). Staff, however, should not, for example, post photographs of private school functions eg. Christmas Party, Summer BBQ. Staff should be aware that they leave themselves open to a charge of professional misconduct if images of a member of staff in a compromising situation are made available on a public profile by anyone. Please refer to the school's '*Safeguarding Policy'* and '*e-safety policy'* as well as the *'Capability and Disciplinary Procedure.'*

Gross misconduct.
Some behaviour is specifically designated as gross misconduct under the School's disciplinary policy and may result in immediate dismissal. Examples of gross misconduct are:

- Sending abusive, rude, illegal, or defamatory messages or material
- Sending a message which could constitute harassment or bullying
- Compiling or distributing chain letters either internally or externally
- Sending confidential information without authorisation
- Excessive personal use (in the opinion of the Head) of school e-mail or school network during term time or holidays
- Introducing a virus to the system by inserting a disk into a School PC or laptop without running a virus check, via e-mail or from down-loading an Internet file
- Misuse of e-mail, the Internet or the system generally which results in a legal claim being made against the School
- Accessing illegal material or pornography on the Internet
- Unauthorised copying or modifying of copyright material or material protected by any other intellectual property right
- Unauthorised downloading of software or files
- Use of the Internet for criminal activity
- Hacking, or other breaches of the Computer Misuse Act 1990
- Misuse of any social media that brings Ashdown House into disrepute

Personal use of equipment
The School tolerates limited personal use of its equipment and the network provided that excessive time is not spent surfing the Internet for non work-related purposes, and there is no interference with the performance of the user's duties and with business use of the network. The School reserves the right to withdraw this facility if the privilege is abused.

Users must not allow School property, for example laptops, projectors, etc to be stolen by not securing it when off School premises (the equipment is clearly expensive in itself, but the information stored on a laptop may be of vital importance to the School).

Remote users

Users will sometimes need to use School equipment and access the School network when working remotely, whether from their home, a non-School site or when travelling. Remote users are reminded that this policy applies to them wherever they are using School equipment and/or accessing the School network, and the following additional regulations also apply.

Users should:

- be particularly careful to secure access to the network by using their password when working from home, in hotels or on trains and planes.

Users should not:

- allow members of their family or anyone else to use the School network or School equipment.
- display confidential information on the screen of their laptop at any time where it may be visible to a non-School employee.

Monitoring

In order to avert as much as possible the risks to the School set out in this policy as well as to avoid abuse and maintain the effectiveness, integrity and security of the school's network the Headmaster will monitor its use. The School's intention is that any monitoring will be proportionate to the risks of harm to the School, and it will be undertaken so as not to intrude on users' privacy only as much as is necessary. Monitoring will be carried out in the same way regardless of whether the user is office based or working remotely.

Any monitoring will be carried out subject to the requirements of legislation including the GDPR 2018.

Network traffic and the performance of the network will be monitored and the School will use a firewall, an anti-virus product, an intrusion detection system and other software to do so.

Specific monitoring and recording of information will be undertaken as follows:

- Internet content and filter management software will be used to control and monitor all internet access.

- anti-virus software will monitor all communications but will only record and quarantine those which it identifies as containing a virus.

- software will monitor the content of e-mails for specific purposes relating to School confidential information.

Access to e-mails
The Head, Bursar or a Trustee of the School may where necessary authorise the opening and reading of a user's e-mails. This will be done in accordance to the monitoring policy stated in the CET handbook. The headmaster receives a copy of all e-mail traffic containing inappropriate material which may constitute a safeguarding concern.

eSafety within the Curriculum

Children will be given more opportunities to develop their digital literacy skills (e.g. sending polite and friendly messages online to other children, the need to create strong passwords etc). They will be shown how to develop a responsible attitude towards searching the World Wide Web and will be reminded of the need to report any concerns they have. The importance of creating strong passwords and the benefits of only joining child-friendly websites will also be taught.

Further up the school, children will now be encouraged to become more independent at researching for information on the World Wide Web, being taught the necessary skills to critically evaluate sites for accuracy and suitability. They will be supported in using online collaboration tools more for communicating and sharing ideas with others, including being taught the need for not revealing personal information to strangers. The aim is to teach them how to manage and deal with risks they encounter by themselves, whilst at the same time encouraging them to become positive users of both new and emerging technologies.

eSafety Training for Staff and Parents

The school understands that everyone has a role to play in empowering children to stay safe while they enjoy new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

For these reasons, the school aims to stay in constant communication with parents about how to enact eSafety policies, what type of education we can offer to either parents or pupils, and to alert each other of specific concerns.

Staff receive regular e-safety training as part of their safeguarding INSET and all staff have access to an online safety course with Educare.

At regular intervals staff and parents receive e-safety awareness training given by Karl Hopwood. For further information pleases visit: http://www.childnet.com/what-we-do/staff-and-trustees/trustees/karl-hopwood

Data Protection

All data held on the school's network is subject to the *GDPR 2018* and the school's *Child Protection Policy*.

Unlicensed or personal software must not be installed on the school's hardware or connected in any way to the school's equipment or systems. If software is deemed to be of use to the school then it should be duly acquired by the school under licence.

Where data of a personal nature such as: school reports, IEPs, correspondence and assessment data is accessed at home via remote login or other by using portable storage media, it must be recognised that this data comes under the *GDPR* and is subject to the school's *Child Protection Policy*. Care must therefore be taken to ensure its integrity and security. Pupils' and others' personal data (ie. Anything which identifies them as individuals) should not be kept on a personal device. Staff should use school machines or use secure remote network access.

Where authorisation has been given to a specific user to use a portable storage medium (e.g. memory stick) it is his/her responsibility to ensure that it does not transmit any viruses onto the school's network. It is recommended that pupils refrain from using such media unattended.

Staff are encouraged to use the 'z' drive on the school network as a central repository for documents such as policy and planning files. Confidential pupil data may be safely stored here as access is only permissible through login by a member of school staff.

The servers containing these networked drives are locked away each night as an extra security measure to prevent against theft.

Data Backups

Data stored on the school's networked drives are backed up regularly so that copies of files may be recovered if the original becomes either lost or damaged.

Responding to Unacceptable Internet Use by Pupils

Pupils should be made aware that all eSafety concerns will be dealt with: promptly, sensitively and effectively so that they will feel able and safe to report any incidents.

The school's DSL and the Headmaster has overall responsibility for Internet safety so any misuse should be reported to them without delay.

Sexting

When people talk about sexting, they usually mean sending and receiving:
•naked pictures or 'nudes'
•'underwear shots'
•sexual or 'dirty pics'
•rude text messages or videos.

They can be sent to or from a friend, boyfriend, girlfriend or someone you've met online.
Sexting can easily happen. Things can go wrong – even when you didn't mean for them to.

Sexting is against the law and is a criminal offence in England and Wales. For further information please see the *Sexual Offences Act 2003* and *Malicious Communications Act 1988*

Depending on the severity and nature of the misuse offence, sanctions will occur in

accordance with the school's *Promoting Good Behaviour Policy* and in consideration of the age of the child.

All incidents should be recorded in the incident file in accordance with the *Child Protection* and *Pupil Behaviour Policies*.

Responding to Unacceptable Internet Use by Staff, Pupils and Visitors

Failure to comply with the *Rules for Responsible Internet Use* could lead to sanctions being imposed and possible disciplinary action being taken, in accordance with the school's *Safeguarding Policy*, *Promoting Good Behaviour Policy* and the law. Misuse should be reported without delay.

Computer Use Policy
Policy statement
The School may provide workstations, laptops, tablets and mobile telephones together with access to e-mail and internet facilities, and may encourage their use wherever it assists job performance. This policy applies to all users IT equipment as well as everyone who has access to the School's network, including employees, visiting staff or outside contractors.

Risks to the School
Whilst use of e-mail and the Internet in particular is often essential for job performance, it exposes the School to risks of legal claims against it including:

- a defamation claim
- a discrimination claim, whether on the grounds of gender, race, disability, sexual orientation, religion or age
- a breach of copyright claim
- a breach of contract claim
- a claim for breach of the duty of confidentiality
- a criminal prosecution following the discovery of child pornography or unlicensed software (for example music files such as MP3's) on the network
- a criminal prosecution or civil action following a breach of data protection legislation

It is for this reason that the School needs to set out in this policy acceptable use expectations and clear rules for the use of the network, the consequences of misuse, and the measures the School will take to monitor compliance with the policy.

School regulations
If a user is at all uncertain or unclear about any of these regulations he or she should discuss them with the Head or the CET Bursar before using the School's network.

Cyber-bullying
Cyberbullying can be carried out using:
Emails
Social network sites
Mobile phones
Text Messages

Instant messenger and chatrooms
Interactive gaming
and sending viruses

Cyberbullying is when one person or a group of people aim to threaten, tease or embarrass someone else by using a mobile phone, the internet or other technologies.

Cyberbullying is no different to any other form of bullying and could lead to some severe sanctions. These could include a fixed term exclusion or expulsion. In some cases this bullying could become a safeguarding issue and could lead to a referral to local authority social care and/or the police.

Please refer to *KCSIE September 2018 Annex C: Online Safety*

Policy Review

This policy is reviewed yearly in conjunction with the *Cothill Educational Trust*, to respond to any significant new developments or legislation in the use of technologies, new threats to eSafety or incidents that have taken place.

This policy is reviewed annually

Reviewed August 2016

Reviewed August 2017

Reviewed July 2018

Reviewed September 2018 (KL/PM)

Advice for this policy may be found at http://www.simonhaughton.co.uk/