Academy Trust

Arden Academy (Arden) is an academy maintained by Arden Multi Academy Trust

Name of Policy	**Online Safety Policy**	
Lead	Nick Burke, Deputy Headteacher	
Governor Committee	Behaviour, Safety, Inclusion & Intervention Committee	
Policy Status	Originally drafted	September 2012
	Governor Approved	YES
	Date Governor Approved	21st October 2024
Review Frequency	1 year	
Version No.	5	
Next Review	Autumn Term 2025	
Reviewed	C Robinson, August 2012	
	On 20th June 2014 – No changes necessary	
	On 16th June 2015 – No changes necessary	
	26th May 2016 (Apply watch/Smart Watch/Google Classroom to be reviewed and written into policy)	
	22nd January 2018 by D Warwood – minor changes to terminology to be approved at next BSII Meeting	
	21st January 2019 – change to lead person	
	September 2020 – minor amendments	
	October 2021 – added Measures to Prevent (pg. 3)	
	Autumn 2022 – Minor changes to terms – no policy changes	
	Autumn 2023 – no policy changes	
	Autumn 2024 – minor changes	

Background/Rationale

Innovative technologies have become integral to the lives of young people today, both within schools and in their lives outside school. The development and expansion of the use of computers, and particularly of the internet, has transformed learning in recent years. Students need to develop high level computer skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that computers can bring to teaching and learning. Schools have made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks."

The purpose of this Online Safety Policy is to ensure that Arden meets its statutory obligations and that students are safe and protected from potential harm, both within and outside school. The policy will also form part of the school's protection from legal challenge, relating to the use of Computers.

The requirement to ensure that students can use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in Arden are bound. The academy Online Safety Policy should help to ensure safe and appropriate use.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. However, the use of these innovative technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to/loss of/sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber bullying.
- Access to unsuitable video/internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the student.

Many of these risks reflect situations in the off-line world and it is important that this Online Safety Policy is used in conjunction with other school policies including the overarching Safeguarding Statement, Child Protection, Data Protection and Whole School Behaviour Policies as well as Acceptable User Guides for both staff and students.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Measures to Prevent

At Arden we recognise that peer on peer abuse may occur or take place online even when not reported. To proactive educate our pupils we have mapped and embedded online safety into our computing curriculums at key stage 3 and 4 as well as our PSHE / CPD and Pastoral curriculums across all key stages. Pupils are also made aware of our support button and who/where they report any concerns they may have about behaviour online. This effective whole school approach to online safety empowers a school to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.
We aim to ensure that children are educated and safeguarded from potentially harmful and inappropriate online material. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.'
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti Phishing Working Group (https://apwg.org/).

Scope of the Policy

This policy applies to all members of the Arden Academy community (including staff, students, volunteers, parents/guardians, visitors, community users) who have access to and are users of academy computer systems, both in and out of academy.

The Education and Inspections Act 2006 empowers the Headteacher/Associate Headteacher, to such extent as is reasonable, to regulate the behaviour of students when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber bullying, or other online safety

related incidents covered by this policy, which may take place out of the academy, but is linked to membership of the academy.

The academy will deal with such incidents within this policy and the Arden Academy Behaviour Policy which includes anti-bullying and will, where known, inform parents/guardians of incidents of inappropriate online behaviour that take place out of the academy.

1. Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety usage of individuals and groups within the school

- Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be conducted by the Governors BSII Committee receiving regular information about online safety incidents and monitoring reports.

Headteacher/Associate Headteacher and Senior Leaders

- The Associate Headteacher is responsible for ensuring the safety (including online safety) of members of the academy
- The Associate Headteacher and Senior Leaders are responsible for ensuring that all relevant staff receive suitable CPD to enable them to conduct their online safety roles and to train other colleagues, as relevant
- The Associate Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see flow chart on dealing with online safety incidents
    - Appendix A, and relevant Academy disciplinary procedures). The procedures for dealing with allegations against staff can be found within the academy Child Protection Policy.

1.1 Network Manager/Technical staff

The Network Manager and Technical support staff are responsible for ensuring:

- that the academy's IT infrastructure is secure and is not open to misuse or malicious attack.
- that the academy meets the online safety technical requirements outlined in the Academy Acceptable Use Policy that users may only access the academy's networks through a properly enforced password protection policy
- the academy's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that they keep up to date with online safety technical information to effectively conduct their online safety role and to inform and update others as relevant.

- that the use of the network/Virtual Learning Environment (GOOGLE CLASSROOM)/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Associate Headteacher or line manager for investigation/action/sanction.
- that monitoring of software and systems are implemented and updated

1.2 Teaching and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices.
- they have read, understood and signed the school Staff Acceptable Use Policy
- they report any suspected misuse or problem to either a Head of Year, member of SLT or the Network Manager and his team as appropriate
- digital communications with students/pupils (email/Virtual Learning Environment (GOOGLE CLASSROOM)/ voice) should be on a professional level and only conducted using official school systems.
- online safety issues are embedded in all aspects of the curriculum and other school activities.
- students/pupils understand and follow the school online safety and acceptable use policy
- students/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor IT activity in lessons, extra-curricular and extended school activities.
- they are aware of online safety issues related to the use of mobile phones, cameras, iPads, smart watches and other hand-held devices and that they monitor their use and implement current school policies regarding these devices.
- in lessons, where internet use is pre-planned, students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

1.3 Designated Safeguarding Lead (DSL)

Will be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data.
- access to illegal/inappropriate materials.
- inappropriate on-line contact with adults/strangers.
- potential or actual incidents of grooming.
- cyberbullying.
- potential for child-on-child abuse

1.4 Students

- Used the school computer systems in accordance with the Student Acceptable Use Policy (AUP), which they and/or their parents/guardians will be expected to sign before being given access to school systems.
- need to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand school policies on the use of mobile phones, smart watches, digital cameras, iPads and other hand-held devices. They should also know and understand school policies on the taking/use of images and on cyber bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

1.5 Parents/Guardians

Parents/Guardians play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and guardians do not fully understand the issues and are less experienced in the use of computers than their children. The school will therefore take every opportunity to help parents understand these issues through newsletters, the school website and information about national/local online safety campaigns/literature. For example, guidance for parents on networking sites – see Appendix B

Parents and guardians will be responsible for:

- endorsing (by signature) the Student Acceptable Use Policy (AUP**)**
- accessing the school website in accordance with the relevant school Acceptable Use Policy.
- ensuring that they themselves do not use the internet/social network sites/other forms of technical communication in an inappropriate or defamatory way

1.6 Community Users

Community Users who access school systems as part of the Extended School provision will be expected to sign an AUP before being provided with access to school systems

2. Teaching and Learning

2.1 Why Internet use is Important

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

2.2 How Internet Use Enhances Learning

The school's Internet access is designed to enhance and extend education.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. In the first instance this will happen in year 7 through computing lessons.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work. This will be taught in a variety of subject areas as and when appropriate.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- A fundamental part of teaching online safety is to check pupil's understanding and knowledge of general personal safety issues. Some pupils may need additional teaching that includes reminders and explicit prompts to link their existing knowledge of "how to keep safe" to the rules that will apply specifically to internet use.

3. Managing Information Systems

3.1 Maintaining Information Systems Security

IT security is a complex issue.

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an antivirus/malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The Network Manager will review system capacity regularly.
- Use of user logins and passwords to access the school network will be enforced

<u>Local Area Network (LAN) security issues include:</u>

- Users must act e.g. the downloading of large files during the working day will affect the service that others receive.

- Users must take responsibility for their network use. For staff, flouting the school Acceptable Use Policy may be regarded as a reason for dismissal.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

Wide Area Network (WAN) security issues include:

- Broadband firewalls and local CPEs (Customer Premises Equipment) are configured to prevent unauthorised access between schools.

- Decisions on WAN security is made on a partnership between schools and the network provider.

3.2 Password Security

The academy will be responsible for ensuring that the academy infrastructure and network is as safe and secure as is reasonably possible. Therefore, a safe and secure username/password system will apply to all academy systems, including email and the GOOGLE CLASSROOM. In addition.

- users can only access data to which they have right of access.
- no user will be able to access another's files, without permission (or as allowed for monitoring purposes within the academy's policies).
- access to personal data will be securely controlled in line with the academy's personal data policy.

The management of password security is the responsibility of the Network Manager

Responsibilities:
All users will have responsibility for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Members of staff will be made aware of the school's password security procedures:

- at induction.
- through the school's Online Safety Policy.
- through the Acceptable Use Agreement.

Students will be made aware of the school's password security procedures:

- in computing lessons
- through the Acceptable Use Agreement

The Network Manager will ensure that full records are kept of:

- User Ids and requests for password changes.
- User log-ons.
- Security incidents related to this policy.

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption. User lists, IDs and other security related information will be given the highest security classification and stored in a secure manner.

3.3 Managing Email

Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits, for example, projects between schools, locally, nationally and as part of the global community.

In the Academy context, email is not considered private, and Arden Academy reserves the right to monitor academy email. However, there is a balance to be achieved between necessary monitoring to maintain the safety of students and staff and the preservation of human rights, both of which are covered by recent legislation. It is important that staff understand they should be using a work provided email account to communicate with parents/guardians, students and other professionals for any official academy business. This is important for confidentiality and security and to safeguard members of staff from allegations.

- Students may only use approved email accounts for school purposes.
- Students must immediately tell a designated safeguarding lead if they receive an offensive email.
- Students must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission from an adult.

- Staff will only use official school provided email accounts to communicate with students and parents/guardians, as approved by the Senior Leadership Team.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.
- Staff should not use personal email accounts during school hours or for professional purposes.
- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored.
- Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents/guardians (email, chat, Google Classroom etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Google Classroom accounts should only be set up using school email addresses.
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to author emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- Spam, phishing and virus attachments can make email dangerous. The school system provider ensures mail is virus checked (ingoing and outgoing), includes spam filtering and backs emails up daily.

3.4 Emailing Personal, Sensitive, Confidential or Classified Information

- e-mailing confidential data is not recommended and should be avoided where possible.
- The use of Windows Live (Hotmail), Gmail or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted.

Where the conclusion is that e-mail must be used to transmit such data, it is essential that staff:

- Obtain express consent from their line manager to provide the information by e-mail
- Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail
- Verify the details, including accurate e-mail address, of any intended recipient of the information.
- Verify (by phoning) the details of a requestor before responding to e-mail requests for information.
- Do not copy or forward the e-mail to any more recipients than is necessary.
- Do not send the information to any person whose details you have been unable to separately verify (usually by phone).
- Send the information as an encrypted document **attached** to an e-mail.
- Provide the encryption key or password by a **separate** contact with the recipient(s).
- Do not identify such information in the subject line of any e-mail.
- Request confirmation of safe receipt.

3.5 Zombie Accounts

Zombie accounts refer to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- The Academy will ensure that all user accounts are disabled once the member of the school has left. This is the responsibility of the Network Manager

3.6 Managing Published Content

- The contact details on the website will be the academy address, email and telephone number. Staff or students' personal information must not be published**.**
- The Associate Headteacher will take overall editorial responsibility for online safety content published by the academy and will ensure that content published is accurate and appropriate.
- The academy website will comply with the academy's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

3.7 Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, students and parents/guardians need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or

longer term. There are many reported incidents of employers conducting internet searches for information about potential and existing employees.

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on academy equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or guardians will be obtained before photographs of students are published on the academy website
- Student's work can only be published with the permission of the student and parents or guardians.

3.8 Managing Social Networking, Social Media and Personal Publishing Sites (Blogs)

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even vastly different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control. For responsible adults, social networking sites provide easy to use, free facilities, although advertising often intrudes, and some sites may be dubious in content. Students should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Examples of social media and personal publishing tools include blogs, wikis, social networking, forums, bulletin boards, multiplayer online safety gaming, chatrooms, instant messenger and many others.

- Students will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for student use on a personal basis.
- Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Students will be advised on security and privacy online safety and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- Student will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Newsgroups will be blocked unless a specific use is approved.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/guardians, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and outlined in the school Staff Acceptable Use Policy – see Appendix F.

3.9 Managing Filtering

Levels of Internet access and supervision will vary according to the student's age and experience. Access profiles must be appropriate for all members of the school community. Older secondary students, as part of a supervised project, might need to access specific adult materials; for instance, a course text or set novel might include references to sexuality. Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily.

Filtering is not 100% effective. There are ways to bypass filters (such as using proxy websites, using a device not connected to the network e.g. smart phone, smart watches). It is therefore important that students are supervised when using internet access and that Acceptable Use Policies are in place. Any material that the school believes is illegal must be reported to appropriate agencies. In addition, Internet

Safety Rules should be displayed, and both children and adults should be educated about the risk's online safety.

Teachers should always evaluate any websites/search engines before using them with their students; this includes websites shown in class as well as websites accessed directly by the students. Often this will mean checking the websites, search results etc. just before the lesson. A site considered safe one day may be changed due to the Internet being a dynamic entity. Particular attention should also be paid to advertisements as they can change each time the web page is accessed.

- The school's broadband access will include filtering appropriate to the age and maturity of students.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all students) will be aware of this procedure.
- If staff or students discover unsuitable sites, the URL will be reported to the Network Manager, who will action the concern as appropriate.
- The school filtering system will block all sites on the Internet Watch Foundation (IWF) list
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies
- Educators will design the school's access strategy to suit the age and curriculum requirements of the students, with advice from network managers.

3.10 Managing Videoconferencing

Videoconferencing, including Zoom, enables users to see and hear each other between separate locations. This 'real time' interactive technology has many uses in education.

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer**.**
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses will not be made available to other sites.
- Videoconferencing contact information will not be put on the school website.
- The equipment must be secure and locked away when not in use.
- School videoconferencing equipment will not be taken off school premises without permission.

- Responsibility for the use of the videoconferencing equipment outside school time will be established with care.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

Users:

- Pupils will ask permission from a teacher before making or answering a videoconference call.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Parents and guardians consent should be obtained prior to children taking part in videoconferences, especially those with endpoints outside of the school.
- Only key administrators should be given access to videoconferencing administration areas or remote-control pages.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content:

- When recording a videoconference lesson, all sites and participants should give written permission. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- Videoconferencing is a challenging activity with a wide range of learning benefits.
    - Preparation and evaluation are essential to the whole activity.
- If third party materials are to be included, check that recording is acceptable to avoid infringing the third-party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class.

3.11 Webcams

- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes, and never using images of children or adults.
- Misuse of the webcam by any member of the school community will result in sanctions.
- Consent is sought from parents/guardians and staff on joining the school, in the same way as for all images.

3.12 Managing Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken on each innovative technology for effective and safe practice in classroom use to be developed. The safest approach is to deny access until a risk assessment has been completed and safety has been established.

The safety and effectiveness of virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the school may be difficult as demonstrated by social networking sites and other online safety tools such as Facebook, YouTube, Skype and Twitter. The registering of individuals to establish and maintain validated electronic identities is essential for safe communication but is often not possible. Video conferencing introduces new dimensions; webcams are increasingly inexpensive and, with faster Internet access, enable video to be exchanged across the Internet. The availability of live video can sometimes increase safety - you can see who you are talking to - but if inappropriately used, a video link could reveal security details.

New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless Internet access. This can offer immense opportunities for learning as well as dangers such as a pupil using a phone to video a teacher's reaction in a demanding situation.

Arden Academy wishes to keep up to date with innovative technologies, including those relating to mobile phones and handheld devices but will need to be ready to develop appropriate strategies, as and when they are considered suitable to support Teaching and Learning.

Emerging technologies will be examined for educational benefit and a risk assessment will be conducted before use in school is allowed.

3.13 Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.

- Secure.
- Only transferred to others with adequate protection.

More detailed information can be found in the School Data Protection Policy.

3.14 Disposal of Redundant Equipment

The WEEE directive came into force, in England, 1st July 2007. It aims to minimise the impact of Waste Electrical and Electronic Equipment on the environment by increasing the re-use and recycling of old computers, electrical equipment, etc. thereby reducing the amount that goes into landfill sites. Manufacturers of electrical and electronic equipment (EEE) now have an obligation to assist with the disposal of waste equipment. For schools this means:

- No equipment can be disposed of through the school's general waste collection process.
- Any computers, or storage media, which may have held personal or confidential data must have their hard drives 'scrubbed' either before or as part of the disposal process. This is to ensure compliance with the Data Protection Act.

WEEE purchased on or after 13th August 2005:
Any WEEE (waste computers, etc.) purchased on or after 13th August 2005, that the Academy wishes to dispose of, is the responsibility of the manufacturer, free of charge. However, there will be a cost for transportation to the 'nominated' collection centre.

WEEE purchased before 13th August 2005:
When purchasing new EEE (computers, etc.) to replace existing equipment that was purchased before 13th August 2005 it is the responsibility of the manufacturer (of the new equipment) to dispose of any items (on a one-to-one basis, e.g. one new computer for one old computer) Free of Charge. There will be a cost for transportation to the 'nominated' collection centre.

When disposing of WEEE purchased before 13th August 2005, that is not being replaced by any new purchase the Academy will need to arrange for its lawful disposal.

- All redundant equipment will be disposed of through an authorised agency. This may include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if

the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.

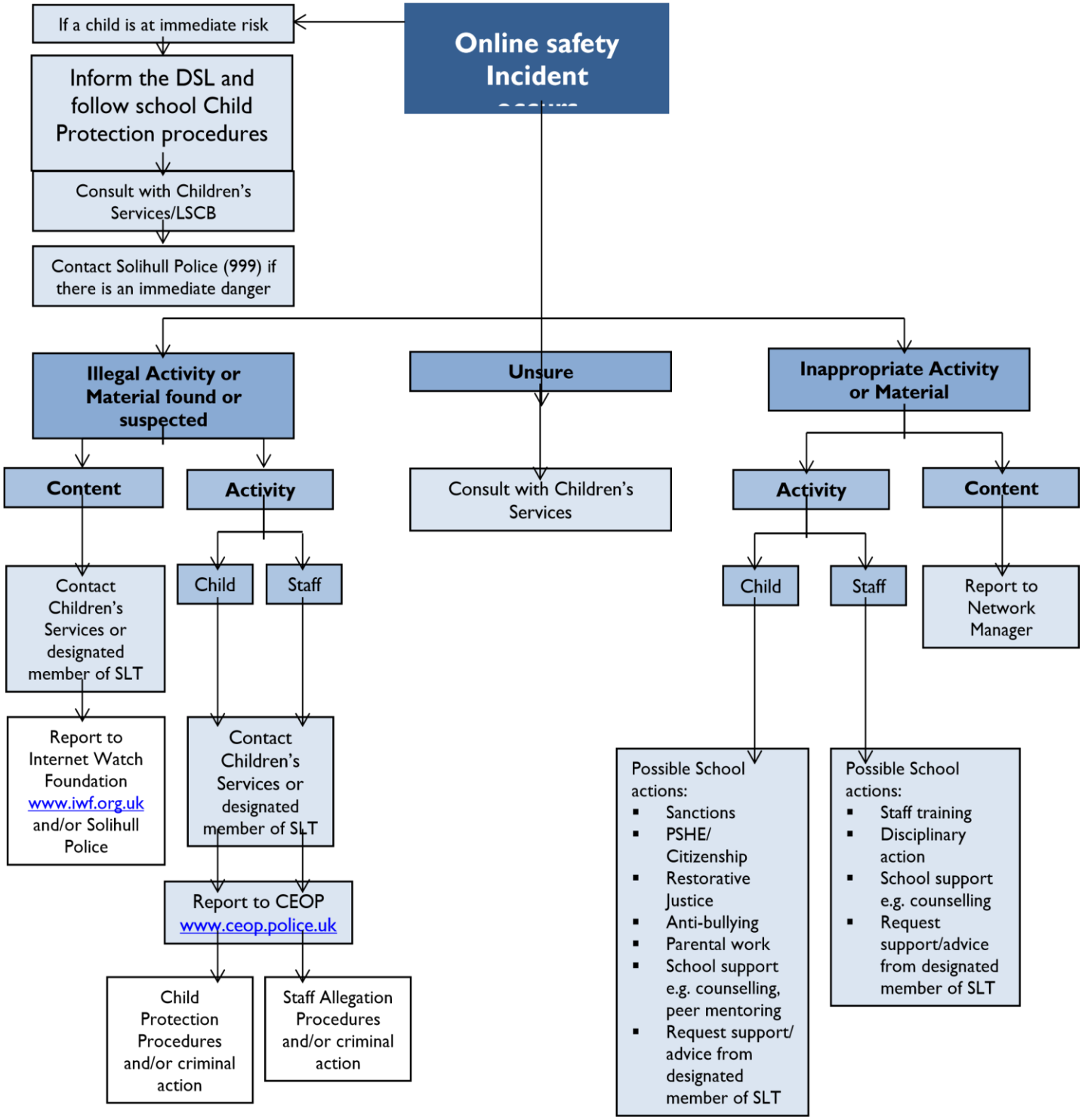
- Disposal of any equipment will conform to:

  - The Waste Electrical and Electronic Equipment Regulations 2013
  - The Waste Electrical and Electronic Equipment (Amendment) Regulations 2018
  - Environment Agency Guidance (WEEE)
  - ICO Guidance – General Data Protection Regulation (GDPR)
  - Electricity at Work Regulations 1989

- The school will maintain a comprehensive inventory of all its IT equipment including a record of disposal.

- Any redundant equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

Appendix A RESPONSE TO AN INCIDENT OF CONCERN



Review school online safety Policies and procedures; record actions in pastoral incident log and implement any changes in the future.

Appendix B SOCIAL NETWORKING SITES GUIDANCE FOR PARENTS/GUARDIANS

There are many children in Years 7 and 8 who have social media Profiles despite the permitted minimum age to use the site being thirteen, according to the site terms and conditions.

Arden Academy is committed to promoting the safe and responsible use of the Internet and as such we feel it is our responsibility to raise this issue as a concern. Whilst children cannot access Facebook or other social networking sites at school, they could have access to it on any other computer or mobile technology. Websites such as Facebook offer amazing communication and social connections, however they are created with their audience in mind, and this is specifically 13 years old. Possible risks for children under 13 using the site may include:

- Facebook use 'age targeted' advertising and therefore your child could be exposed to adverts of a sexual or other inappropriate nature, depending on the age they stated they were when they registered.
- Children may accept 'friend requests' from people they do not know in real life which could increase the risk of inappropriate contact or behaviour.
- Language, games, groups and content posted or shared on Facebook is not moderated, and therefore can be offensive, illegal or unsuitable for children.
- Photographs shared by users are not moderated and therefore children could be exposed to inappropriate images or even post their own.
- Underage users might be less likely to keep their identities private and lying about their age can expose them to further risks regarding privacy settings and other options.
- Facebook could be exploited by bullies and for other inappropriate contact.
- Facebook cannot and does not verify its members therefore it important to remember that if your child can lie about who they are online with, so can anyone else!

We feel that it is important to point out the risks of underage use of such sites, so you can make an informed decision as to whether to allow your child to have a profile or not. These profiles will have been created away from school and sometimes by a child, their friends, siblings or even parents. We will act (such as reporting aged profiles) if a problem comes to our attention that involves the safety or wellbeing of any of our students.

Should you decide to allow your children to have a social media profile we strongly advise you to:

- Check their profile is set to private and that only 'friends' can see information that is posted.
- Monitor your child's use and talk to them about safe and appropriate online safety behaviour such as not sharing personal information and not posting offensive messages or photos.
- Ask them to install the CEOP (Child Exploitation and Online safety Protection Centre) application from www.facebook.com/clickceop on their profile. This places a bookmark

on their profile to CEOP and the 'Report Abuse' button which has been known to deter offenders.

- Have a look at the advice for parents/guardians from Facebook www.facebook.com/help/?safety=parents;
- Set up your own profile so you understand how the site works and ask them to add you as a friend on their profile so you can keep track of what they are posting online safety.
- Make sure your child understands the following rules:

  - Always keep your profile private.
  - Never accept friends you do not know in real life.
  - Never post anything which could reveal your identity.
  - Never post anything you would not want your parents to see.
  - Never agree to meet someone you only know online without telling a trusted adult;
    - Always tell someone if you feel threatened or someone upsets you.

We recommend that all parents/guardians visit the CEOP ThinkUKnow website for more information

Appendix C

Staff Acceptable Use Policy

Guidelines for Staff

Arden Academy has provided computers for use by staff as a valuable tool for teaching, learning, and administration of the academy. Use of Arden Academy computers, by both members of staff and pupils, is always governed by the following policy. Please ensure you understand your responsibilities under this policy and direct any questions or concerns to the IT Network Manager in the first instance.

All members of staff have a responsibility to use the Arden academy's computer system in a professional, lawful, and ethical manner. Deliberate abuse of the academy's computer system may result in disciplinary action (including termination), and civil and/or criminal liability.

Please note that use of the academy network is intended to be as permissive and flexible as possible under current UK legislation and DfE guidelines. This policy is not intended to arbitrarily limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of Arden Academy and staff, to safeguard the reputation of the academy, and to ensure the safety of all users. Please respect these guidelines, many of which are in place for your protection.

Lastly, Arden academy recognises that the distinction between computer use at work and at home is increasingly blurred, with many of us now using our own computers for work. While the academy neither wishes nor intends to dictate how you use your own computer, staff should consider that the spirit of this policy applies whenever you are undertaking an activity that stems from your employment with the academy.

Computer Security and Data Protection

- You will be provided with a personal account for accessing the computer system, with your own username and password. This account will be tailored to the level of access you require and is for your use only. As such, **you must not disclose your password to anyone**, including IT support staff. If you do so, you will be required to change your password immediately.
- You **must not allow a pupil to have individual use of a staff account** under any circumstances, for any length of time, even if supervised.
- When leaving a computer unattended, you **must** ensure you have either logged off your account or locked the computer to prevent anyone using your account in your absence.
- You **must not** store any sensitive or personal information about staff or students on any portable storage system (such as a USB memory stick, portable hard disk, or personal computer) unless that storage system is encrypted and approved for such use by Arden Academy.

- You **must not** transmit any sensitive or personal information about staff or students via email without the data being encrypted by a method approved by Arden Academy.
- When publishing or transmitting non-sensitive material outside of Arden academy, you **must** take steps to protect the identity of any pupil whose parents have requested this.
- If you use a personal computer at home for work purposes, you **must** ensure that any Arden Academy related sensitive or personal information is secured to prohibit access by any non-member of staff and encrypted to protect against theft.

- You **must** make your own backup of data kept on any storage system other than the network storage drives or your 'My Documents' folder. This includes USB memory sticks (even those owned or issued by the academy) or a personal computer.
- You **must** ensure that items of portable computer equipment (such as laptops, i-pads, digital cameras, flip cameras or portable projectors) are securely stored in a locked room or cupboard when left unattended.
- Equipment taken offsite is not routinely insured by the academy. If you take any Arden Academy computer equipment offsite, you should ensure that adequate insurance cover has been arranged to cover against loss, damage, or theft.
- Where i-pads have been issued you must not change the security settings and should not synchronise them with your personal settings, music, photographs or videos

Personal Use

Arden academy recognises that occasional personal use of the academy's computers is beneficial both to the development of your IT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use

- **must** comply with all other conditions of this AUP as they apply to non-personal use, and all other academy policies regarding staff conduct.
- **must not** interfere in any way with your other duties or those of any other member of staff.
- **must not** have any undue effect on the performance of the computer system; and
- **must not** be for any commercial purpose or gain unless explicitly authorised by Arden academy.

Personal use is permitted at the discretion of Arden Academy and can be limited or revoked at any time.

Use of your own Equipment

- Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff

and **must not** be used until approved. This test must be performed at regular intervals as required by Arden academy's normal rules on electrical safety testing.

- You **must not** connect personal computer equipment to Arden academy computer equipment without prior approval from IT Network staff, except for storage devices such as USB memory sticks.
- If you keep files on a personal storage device (such as a USB memory stick), you **must** ensure that other computers you connect this storage device to (such as your own computers at home) have an up-to date anti-virus system running to protect against the proliferation of harmful software onto the academy computer system.

Conduct

- You **must** always conduct your computer usage professionally, which includes being polite and using the system in a safe, legal and business appropriate manner. Among uses that are considered unacceptable are the following:
    - Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials.
    - Making ethnic, sexual-preference, or gender-related slurs or jokes.
- You **must** respect, and not attempt to bypass, security or access restrictions in place on the computer system.
- You **must** not intentionally damage, disable, or otherwise harm the operation of computers.
- You **must** make efforts not to intentionally waste resources. Examples of resource wastage include:
    - Excessive downloading of material from the Internet.
    - Excessive storage of unnecessary files on the network storage areas.
- Use of computer printers to produce class sets of materials, instead of using photocopiers.

- You should avoid eating or drinking around computer equipment.

Use of Social Networking websites and online forums

Staff must take care when using social networking websites, even when such use occurs in their own time using their own computer. Social Networking sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children.

You must not allow any pupil to access personal information you post on a social networking site. In particular:

- You **must not** add a pupil to your 'friends list.'
- You **must** ensure that personal information is not accessible via a 'Public' setting, but ensure it is set to a 'Friends only' level of visibility.

- You should avoid contacting any pupil privately via a social networking website, even for Arden Academy related purposes.
- You should take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them access to your personal information.

Staff should also take care when posting to any public website (including online safety discussion forums or blogs) that their comments do not harm their professional standing or the reputation of Arden Academy – even if their online safety activities are entirely unrelated to Arden Academy.

- Unless authorised to do so, you **must not** post content on websites that may appear as if you are speaking for the academy.
- You should not post any material online safety that can be clearly linked to the academy that may damage Arden Academy's reputation.
- You should avoid posting any material clearly identifying yourself, another member of staff, or a pupil, which could potentially be used to embarrass, harass, or defame the subject.

Use of Email

All members of staff with a computer account are provided with an email address for communication both internally and with other email users outside the academy. The following considerations must be made when communicating by email:

- E-mail has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in the same way. Copies of e-mails may therefore have to be made available to third parties. You **must** be cautious when sending both internal and external mails. The professional standards that apply to internal memos and external letters must be observed for e-mail.

E-mail to outside organisations has the same power to create a binding contract as hardcopy documents. Check e-mail as carefully as written contracts, always use a spell checker and, where appropriate, obtain legal advice before sending. You **must not** purchase goods or services on behalf of the academy via e-mail without proper authorisation.

- All academies e-mail you send should have a signature containing your name, job title and the name of the Arden academy.
- E-mail is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, you **must not** send, transmit, or otherwise distribute proprietary information, copyrighted material, trade secrets, or other confidential information belonging to the academy.
- Having an external e-mail address may lead to receipt of unsolicited e-mail containing offensive and/or sexually explicit content. The academy will take measures to minimise the receipt and impact of such content but cannot be held responsible for material viewed or received by users from the Internet.

- You must not send chain letters or unsolicited commercial e-mail (also known as SPAM).

Supervision of Pupil Use

- Pupils **must** be always supervised when using academy computer equipment. When arranging use of computer facilities for pupils, you must ensure supervision is available.
- Supervising staff are responsible for ensuring that the separate Acceptable Use Policy for pupils is enforced.
- Supervising staff **must** ensure they have read and understand the separate guidelines on online safety, which pertains to the child protection issues of computer use by pupils.

Privacy

- Use of the academy computer system, including your email account and storage areas provided for your use, may be subject to monitoring by the academy to ensure compliance with this Acceptable Use Policy and applicable laws. This may include remote monitoring of an interactive logon session. In particular, the academy does keep a complete record of sites visited on the Internet by both pupils and staff, however, usernames and passwords used on those sites are NOT monitored or recorded.
- You should avoid storing sensitive personal information on the academy computer system that is unrelated to academy activities (such as personal passwords, photographs, or financial information).
- The academy may also use measures to audit use of computer systems for performance and diagnostic purposes.
- **Use of the Arden Academy computer system indicates your consent to the above-described monitoring taking place.**

Confidentiality and Copyright

- Respect the work and ownership rights of people outside the academy, as well as other staff or pupils.
- You are responsible for complying with copyright law and licenses that may apply to software, files, graphics, documents, messages, and other material you wish to use, download or copy. Even if materials on the academy computer system or the Internet are not marked with the copyright symbol (©), you should assume that they are protected under copyright laws unless there is an explicit permission on the materials to use them.

  You **must** consult a member of IT Network staff before placing any order of computer hardware or software, or obtaining and using any software you believe to be free. This is to check that the intended use by the academy is permitted under copyright law (as well as to check compatibility and discuss any other implications that the purchase may have). Do not rely on the claims of suppliers, who do not have specific knowledge of the academy's systems.
- As per the standard staff contract, any invention, improvement, design, process, information, copyright work, trade mark or trade name made, created or discovered by you during the course of your employment in any way affecting or relating to the

business of the academy or capable of being used or adapted for use within the academy shall be immediately disclosed to the academy and shall to the extent permitted by law belong to and be the absolute property of the academy.

- By storing or creating any personal documents or files on the academy computer system, you grant the academy a non-exclusive, universal, perpetual, irrevocable, and royalty-free license to use, copy, and distribute those documents or files in any way the academy sees fit.

Reporting Problems with the Computer System

It is the job of the IT Network Manager to ensure that the Arden academy computer system is always working optimally and that any faults are rectified as soon as possible. To this end:

- You should report any problems that need attention to a member of IT support staff as soon as is feasible. Problems that seriously hinder your job or teaching and require immediate attention should be reported by telephone; any other problem **must** be reported via the Online Safety Support Request system.
- If you suspect your computer has been affected by a virus or other malware, you **must** report this to a member of IT Network staff **immediately**.
- If you have lost documents or files, you should report this as soon as possible. The longer a data loss problem goes unreported, the lesser the chances of your data being recoverable (mere minutes can count).

Reporting Breaches of this Policy

All members of staff have a duty to ensure this Acceptable Use Policy is followed. You must immediately inform a member of the IT Network staff, or the Headteacher, of abuse of any part of the computer system. You should report:

- any websites accessible from within academy that you feel are unsuitable for staff or student consumption.
- any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, ps, etc.
- any breaches, or attempted breaches, of computer security; or
- any instance of bullying or harassment suffered by you, another member of staff, or a pupil via the academy computer system.

Reports should be made either via email or the Online Safety Support Request system. All reports will be treated confidentially.

Review and Evaluation

This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff.

Notes

1. "Sensitive personal information" is defined as information about an individual that is protected by law under the Data Protection Act 1998. Examples of such data include addresses and contact details of individuals, dates of birth, and pupil SEN data. This list is not exhaustive. Further information can be found in the Arden Academy's Data Protection Policy.

I agree to abide by the above
Name:
Date:
Department:

Appendix D

Acceptable User Policy for Students

I know that I must use the computers safely

- I know that Arden Academy can remotely monitor what I do on the computers.
- I will treat my username and password sensibly – I will not let anyone else use it, and I will not use theirs.
- I will be aware of my personal safety when I am communicating online safety and will not share personal information about myself or others.
- If I arrange to meet someone that I have communicated with online safety, I will do so in a public place and take an adult with me.
- I will tell a member of staff immediately about any unpleasant or inappropriate material or messages on the computer, or anything that makes me feel uncomfortable when I see it.
- I understand that Arden Academy will look after me and my peers and can help if anything happens online– even if I am using a computer at home.

I know that I must use the computers responsibly

- I understand that the computers are here for Arden Academy work, and I will only play games on them or use them for personal use if I have permission.
- I will only upload pictures or videos from inside the Arden academy if I have permission.
- I understand that the academy's security and Internet filter is there to protect me, and protect the computer network, and I will not try to bypass it. If I need access to a blocked website, I will ask my teacher.
- I will only download music or videos onto the computer if it is related to my Arden academy work.
- I understand that I must not download or display inappropriate pictures or other material from the Internet.

I know that I must help look after the computers

- If I have a problem with my computer, I will tell a teacher immediately so that the problem can be fixed – I will not leave it broken for the next person.
- I will only use programs that are already on the Academy computer. If I need a new program, I will ask my teacher - I will not try to install it myself.
- I will not try to connect my own computer or mobile phone to the network.
- I will only change settings on the computer if I am allowed to do so – I will not try to change anything that might cause the computer to go wrong.
- I know that food and drink is not allowed in the computer rooms, and that I should not eat or drink around any computer.

I know that I must respect others when using the computers

- I will always treat others the same way I would want them to treat me – just as I would when not using the computers. I will not use the computers to harass or bully anyone.
- I will be polite online safety, and I will not use strong, aggressive, or inappropriate language. I appreciate that others may have different opinions.
- I will not take or distribute pictures or videos of anyone without their permission.

iPad Acceptable Use Policy

I understand that each iPad is the property of Arden Academy, and I may use the iPads during lessons and under the supervision of teachers.

I must **not**:

- Remove the school-supplied case
- Apply any stickers or decorations to the iPad
- Use the iPad to access any inappropriate material, as defined by the network acceptable use policy
- Use the iPad camera function inappropriately
- Attempt to modify the iPad hardware in any way, including jailbreaking
- Add or remove applications from the iPad
- Create an iTunes account on the iPad
- Change any configuration settings on the iPad, particularly network configuration
- Clear their browser history, except as directed to by staff
- Change or disable the access password on the iPad
- Drop or place heavy objects (books, laptops, etc) on top of the iPad (The iPad screen is made of glass and therefore is subject to cracking and breaking if misused)
- Clean the iPad's screen with anything other than a soft cloth or approved laptop screen cleaning solution provided by the school
- Remove the iPad from a classroom without permission (iPads must always be returned to the iPad trolley/the Librarian / member of staff after use)

I understand that the Arden Academy IT technical staff will occasionally monitor iPad wireless activity. The academy reserves the right to access files and communications without warning to ensure that the facilities are not being misused.

Accidental Damage or Negligence

I understand that if the iPad that I have been using had been intentionally or negligently damaged, then I may be liable for the cost of repair or replacement. Therefore, if on receiving an iPad to use I see that it has been damaged I will immediately report it to my teacher.

I agree to abide by the above
Name:
Date:
Form:

Appendix E RESPONSIBLE INTERNET USE

Arden Academy Rules for Staff and Students

- The school owns the computer system. This Responsible Internet Use statement helps to protect students, staff and the school by clearly stating what use of the computer resources is acceptable and what is not.
- Irresponsible use may result in the loss of Internet access. Network access must be made via the user's authorised account and password, which must not be given to any other person.
- School computer and Internet use must be appropriate to the student's education or to staff professional activity. Copyright and intellectual property rights must be respected.
- E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.
- Users are responsible for e-mail they send and for contacts made. Anonymous messages and chain letters are not permitted.
- The use of chat rooms is not allowed.
- The school IT systems may not be used for private purposes, unless the Headteacher/Associate Headteacher has given permission for that use.
- Use for personal financial gain, gambling, political purposes or advertising is not permitted. ▪
- IT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.
- The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
- Irresponsible use may result in the loss of Internet access. Network access must be made via the user's authorised account and password, which must not be given to any other person.
- School computer and Internet use must be appropriate to the student's education or to staff professional activity. Copyright and intellectual property rights must be respected.
- E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.
- Users are responsible for e-mail they send and for contacts made.
- Anonymous messages and chain letters are not permitted.
- The use of chat rooms is not allowed.
- The school IT systems may not be used for private purposes, unless the Associate Headteacher has given permission for that use.
- Use for personal financial gain, gambling, political purposes or advertising is not permitted.
- IT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.

ONLINE SAFETY LINKS

The following links may help those who are developing or reviewing a school Online Safety Policy.

- **CEOP (**Child Exploitation and Online safety Protection Centre): Click here to access
- **Childline**: Click here to access
- **Childnet**: Click here to access
- **Click Clever Click Safe Campaign**: Click here to access
- **Cybermentors**: Click here to access
- **Digizen**: Click here to access
- **Internet Watch Foundation (IWF)**: Click here to access
- **Solihull Local Safeguarding Children Board (Solihull LSCB) www.solihull.gov.uk/staysafe**
- **Kidsmart**: Click here to access
- **Teach Today**: Click here to access
- **Think U Know website**: Click here to access
- **Virtual Global Taskforce — Report Abuse**: Click here to access
- **Orange Education**: Click here to access
- **Safe**: Click here to access
- **Information Commissioner's Office (ICO)** Click here to access
- **INSAFE** Click here to access
- **National Education Network (NEN)** Online safety Audit Tool: Click here to access
- **Anti-Bullying Network** - Click here to access
- **Cyberbullying.org** - Click here to access
- **Ofcom Report:** Click here to access
- **Learning Curve Education:** Click here to access
- **UK Safer Internet Centre:** Click here to access
- **UK Council for Child Internet Safety (UKCCIS):** Click here to access
- **Wise Kids:** Click here to access
- **Teacher Tube:** Click here to access
- **Teach Today:** Click here to access
- **Beat Bullying:** Click here to access
- **BBC Teachers:** Click here to access
- **Grid Club**: Click here to access
- **Team:** Click here to access
- **Sites for Teachers:** Click here to access
- **DfE:** Click here to access
- **Know the Net:** Click here to access
- **Family Online safety Institute:** Click here to access
- **e-safe Education**: Click here to access

- **Facebook Advice to Parents:** Click here to access
- **Record Management Society:** Click here to access
- **Test your online safety skills:** Click here to access

BECTA publications *(saved from the National Archives since BECTA's closure in 2011)* Some of BECTA's guidance documents include:

- Online safety - Click here to access
- Safeguarding Children Guide - - Click here to access
- Safeguarding Children Checklist - Click here to access
- LSCB Strategy - Click here to access
- Online safety Behaviours - Click here to access
- Safeguarding Learners - Click here to access

Irresponsible use may result in the loss of Internet access. Network access must be made via the user's authorised account and password, which must not be given to any other person.

School computer and Internet use must be appropriate to the student's education or to staff professional activity. Copyright and intellectual property rights must be respected.

E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.

Users are responsible for e-mail they send and for contacts made.

- **Anonymous messages and chain letters are not permitted.**
-
- ▪
- **The use of chat rooms is not allowed.**
-
- ▪
- **The school IT systems may not be used for private purposes, unless the Headteacher/Associate Headteacher has given permission for that use.**
-
- ▪
- **Use for personal financial gain, gambling, political purposes or advertising is not permitted.**
-
- ▪

IT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.

Appendix F LEGAL FRAMEWORK

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of eighteen. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo photographs

(digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Criminal Justice Act 2003
Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of eighteen. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming is committed if you are over eighteen and have communicated with a child under sixteen at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under sixteen to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under eighteen, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc. fall in this category of trust).

Any sexual intercourse with a child under the age of thirteen commits the offence of rape.

N.B. Schools should have a copy of The Home Office "Children & Families: Safer from Sexual Crime" document as part of their child protection packs. Click here to access.

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or

persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent there is no need to prove any intent or purpose.

Data Protection Act 2018
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection

The Computer Misuse Act
1990 (sections 1 - 3) This Act
makes it an offence to:

- Erase or amend data or programs without authority.
- Obtain unauthorised access to a computer.
- "Eavesdrop" on a computer.
- Make unauthorised use of computer time or facilities; ✦ Maliciously corrupt or erase data or programs; ✦ Deny access to authorised users.

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose were to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is

usually the copyright owner, but if it was created during employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually, a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly like an existing Mark.

Public Order Act 1986 (sections 17 — 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they must follow several set procedures.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, to:

- Establish the facts.
- Ascertain compliance with regulatory or self-regulatory practices or procedures.

- Demonstrate standards, which are or ought to be achieved by persons using the system.
- Investigate or detect unauthorised use of the communications system.
- Prevent or detect crime or in the interests of national security.
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible to:
- Ascertain whether the communication is business or personal.
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Criminal Justice and Immigration Act 2008

Section 63 offence to possess "extreme pornographic image"

33

63 (6) must be "grossly offensive, disgusting or otherwise obscene"

63 (7) this includes images of "threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead" must also be "explicit and realistic". Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyberbullying/ Bullying:

- Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site.
- School staff can confiscate items such as mobile phones etc. when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/antibullying policy.

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Human Rights Act 1998

This does not deal with any issue specifically or any discrete subject area within the law. It is a type of "higher law," affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial.
- The right to respect for private and family life, home and correspondence.
- Freedom of thought, conscience and religion.
- Freedom of expression.
- Freedom of assembly.
- Prohibition of discrimination.
- The right to education.

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

Appendix G – Glossary of Terms

AUP	Acceptable Use Policy – see templates earlier in this document
CEOP	Child Exploitation and Online safety Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CLEO	The Regional Broadband Consortium of Cumbria and Lancashire – is the provider of broadband and other services for schools and other organisations in Cumbria and Lancashire
CPD	Continuous Professional Development
DfE	Department for Education
ECM	Every Child Matters
FOSI	Family Online Safety Institute
HSTF	Home Secretary's Task Force on Child Protection on the Internet
ICO	Information Commissioners Office
COMPUTING	Information and Communications Technology
Computing Mark	Quality standard for schools provided by Naace
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
JANET	Provides the broadband backbone structure for Higher Education and for the National Education Network.

KS1	Key Stage 1 (2, 3, 4 or 5) – schools are structured within these multiple age groups e.g. KS3 = years 7 to 9 (age 11 to 14)
LA	Local Authority
LAN	Local Area Network
Learning Platform	A learning platform brings together hardware, software and supporting services to support teaching, learning, management and administration.
LSCB	Local Safeguarding Children Board
MIS	Management Information System
MLE	Managed Learning Environment
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. CLEO in Cumbria) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
Ofsted	Office for Standards in Education, Children's Services and Skills
PDA	Personal Digital Assistant (handheld device)
PHSE	Personal, Health and Social Education
RBC	Regional Broadband Consortia (e.g. CLEO) have been established to procure broadband connectivity for schools in England. There are 13 RBCs covering most local authorities in England, Wales and Northern Ireland.
SEF	Self-Evaluation Form – used by schools for self-evaluation and reviewed by Ofsted prior to visiting schools for an inspection
SRF	Self-Review Form – a tool used by schools to evaluate the quality of their IT provision and judge their readiness for submission for the Computing Mark
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
URL	Uniform Resource Locator (URL) it is the global address of documents and other resources on the World Wide Web.

GOOGLE CLASSROOM Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

WAP Wireless Application Protocol