THE AVON VALLEY SCHOOL AND PERFORMING ARTS COLLEGE

ONLINE SAFETY POLICY

Date of Policy: November 2022

Date of next review: November 2023

Who the review will involve: Head Teacher, IT Manager, Governors, Senior Leadership Team, Staff.

Senior member of staff responsible for overseeing that this policy is implemented and regularly reviewed: Laura Bindley (Assistant Headteacher and DSL)

ONLINE SAFETY POLICY STATEMENT

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.
- The policy statement applies to all staff, volunteers, children and young people and anyone involved in Avon Valley School's activities.

The Legal Framework

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on:

- online abuse
- bullying
- child protection.

We believe that:

- children and young people should never experience abuse of any kind
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- the online world provides everyone with many opportunities; however, it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and young people safe online, whether or not they are using The Avon Valley School's network and devices
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety

- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

Find out more about:

safeguarding children who come from Black, Asian and minoritised ethnic communities

safeguarding d/Deaf and disabled children and young people

safeguarding LGBTQ+ children and young people

safeguarding children with special educational needs and disabilities (SEND)

We will seek to keep children and young people safe by:

- appointing an online safety coordinator, Mrs Charlotte Gore
- providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults
- supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- supporting and encouraging parents and carers to do what they can to keep their children safe online
- developing an online safety agreement for use with young people and their parents or carers
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child or young person
- reviewing and updating the security of our information systems regularly
- ensuring that user names, logins, email accounts and passwords are used effectively
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- providing supervision, support and training for staff and volunteers about online safety
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term

Related policies and procedures

This policy statement should be read alongside our organisational policies and procedures, including:

- Safeguarding and child protection
- Behaviour
- Professional code of conduct for staff and volunteers
- Anti-bullying policy and procedures
- Photography and image sharing guidance

DEVELOPMENT AND DISSEMINATION PROCESS

This policy was formulated by a working party consisting of the Faculty Leader for Business, Computing and Media, the IT Manager, the Deputy Headteacher and the DSL.

AIMS

The purpose of the Online Safety policy at Avon Valley School, is to protect all users of ICT and online use both within school and at home and to raise awareness of the safety issues associated with information systems and electronic communications as a whole. It also includes education on the risks and responsibilities of using communication technology and provides a statutory duty of care for those working with children in school.

PRINCIPLES, VALUES AND ENTITLEMENTS

1.1 Why have an online safety policy?

Students interact with the internet and other communications technologies such as mobile phones on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas and social interaction are both greatly beneficial, but can occasionally place young people in danger.

Online safety comprises all aspects relating to children and young people and their safe use of the internet, mobile phones, gaming and other technologies, both in and out of school. It includes education on risks and responsibilities and is part of the duty of care which applies to everyone working with children. A new national online safety drive is being led by the Child Exploitation and Online Protection Centre (CEOP). It is important to ensure that our students have a strong understanding of their responsibilities and the risks of the use of online systems.

1.2 What is online safety?

The Warwickshire Schools online safety policy reflects the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole, including the rise of online gaming communication and gambling awareness.

Online safety encompasses not only internet technologies but also, gaming and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology and online systems providing safeguards and awareness for users to enable them to control their online experiences.

The internet is an open communications channel, available to all. Applications such as web browsers, e-mail clients, blogs, online gaming and social networking all transmit information via the internet to global destinations. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the internet make it an invaluable resource used by millions of people every day.

Some of the material on the internet is published for an adult audience and is unsuitable for students. For instance, there is information on weapons, crime and racism that would be more restricted elsewhere. It is important that students are made aware of appropriate behaviour in relation to contacting others and they must also understand that publishing personal information could compromise their own, and others peoples, security. Gaming and online live gaming systems allows for live gambling activities encouraging children to use virtual money and real money to purchase against risk.

SCHOOL STAFF

Any allegation of inappropriate behaviour by anyone using the internet or online systems should be reported to senior management and investigated with great care - an innocent explanation may exist. In particular, allegations against members of staff will be investigated using the recommended WCC procedures.

Email, text messaging, instant messaging software and online and live gaming messaging all provide additional channels of communication between staff and students and inappropriate behaviour can occur. Staff should appreciate the power and extent of the Police's technical capabilities to identify the sender of inappropriate messages. AVS uses school-owned phone and school support emailing systems for staff-student contact to enable monitoring and to protect staff from false accusations.

ONLINE SAFETY FOR STUDENTS WITH ADDITIONAL NEEDS

There is an underlying assumption that children understand the application of online safety. Students need to understand that rules given to them must be followed. Students must learn safety rules in a way that does not frighten them and which gives them confidence to know what to do in certain situations. Students must understand that certain rules will change and develop as they get older and must learn how to apply strategies that will help them to avoid certain risks.

The school SENCO will be involved in coordinating advice between ICT specialist and support staff.

This may take the form of student-focused strategies that would apply to a student with specific needs that would need to be available to all staff implicated in internet use with that student.

ROUTE TO ONLINE SAFETY – SECONDARY

The online safety policy will work in conjunction with other policies including the behaviour policy, anti-bullying and curriculum.

The online safety policy considers:

1. Guided educational use

Our curriculum supports the safe use of the internet as it produces significant educational benefits including access to information from around the world and the ability to communicate widely and to publish easily. Within our curriculum the internet used should be planned, task-orientated and educational within a regulated and managed environment in order to enrich

and extend learning activities. Directed and successful internet use will also reduce the opportunities for activities of dubious worth. Staff will guide students in online activities that will support the learning outcomes planned for the students' age and maturity.

2. Risk Assessment

21st century life presents dangers including bullying, violence, racism, exploitation and gambling from which children and young people must be protected. At an appropriate age they must learn to recognise and avoid these risks to become "wise online".

AVS will perform risk assessments to ensure that the staff are fully aware of, and can mitigate risks of, internet use. Students must know how to cope if they encounter inappropriate material.

Students' internet access may be provided in youth clubs, libraries, public access points and in homes. Students will be given advice on how to manage their use of the internet in these places, as well as on the range of devices which has internet access.

3. Responsibility

Online safety relies on staff, schools, governors, advisers and, in particular, parents and the students themselves taking responsibility. Staff have a particular responsibility to educate, supervise, use, plan, access and set good examples. The balance between educating students to take a responsible approach and the use of regulation must be judged carefully and assessed regularly due to fast changing and developing online technologies.

LEADERSHIP AND MANAGEMENT OF ONLINE SAFETY

1. The person responsible for Online safety in the school is the Designated Safeguard Leader (DSL) or the Deputy DSL. The DSL will liaise with the IT Manager, Faculty Leader of Business, Computing and Media and the Deputy Head with responsibility for whole school ICT as necessary.

2. Teachers are to remain vigilant at all times in their classrooms when using communication technologies and to report incidents required by the policy.

3. Response to an incident of concern must be dealt with immediately following the guidelines in the policy.

Risks to online safety are caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to students and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to occasional extremely concerning incidents.

This section will help staff determine what action they can take and when to report an incident of concern to the school Designated Safeguarding Lead.

2.1 **What does electronic communication include?**

Electronic communication includes, but is not limited to:

- Internet collaboration tools: social networking sites, blogs, Google Classroom social networking applications and online gaming systems.

- Internet research: web sites and search engines
- Mobile phones, iPads and tablets
- Internet communications: e-mail and instant messaging applications
- Webcams and video conferencing
- Games consoles

2.2 **Social Media usage by the school**

As a school we use social media platforms to share information with the public (mainly parents and students). The school currently uses Facebook, Twitter and Instagram as a way to share information and events around the school, as well as a form of advertisements when there are job vacancies.

The use of social media within the school is managed by the extended leadership team, who check the permission status before publishing any names or images of students and staff. They also manage the suitability of posts and manage the language which is used when publishing information publicly.

As a school the use of sharing information via social media platforms is done with care, consideration and sensitivity, which allows for successful sharing of information.

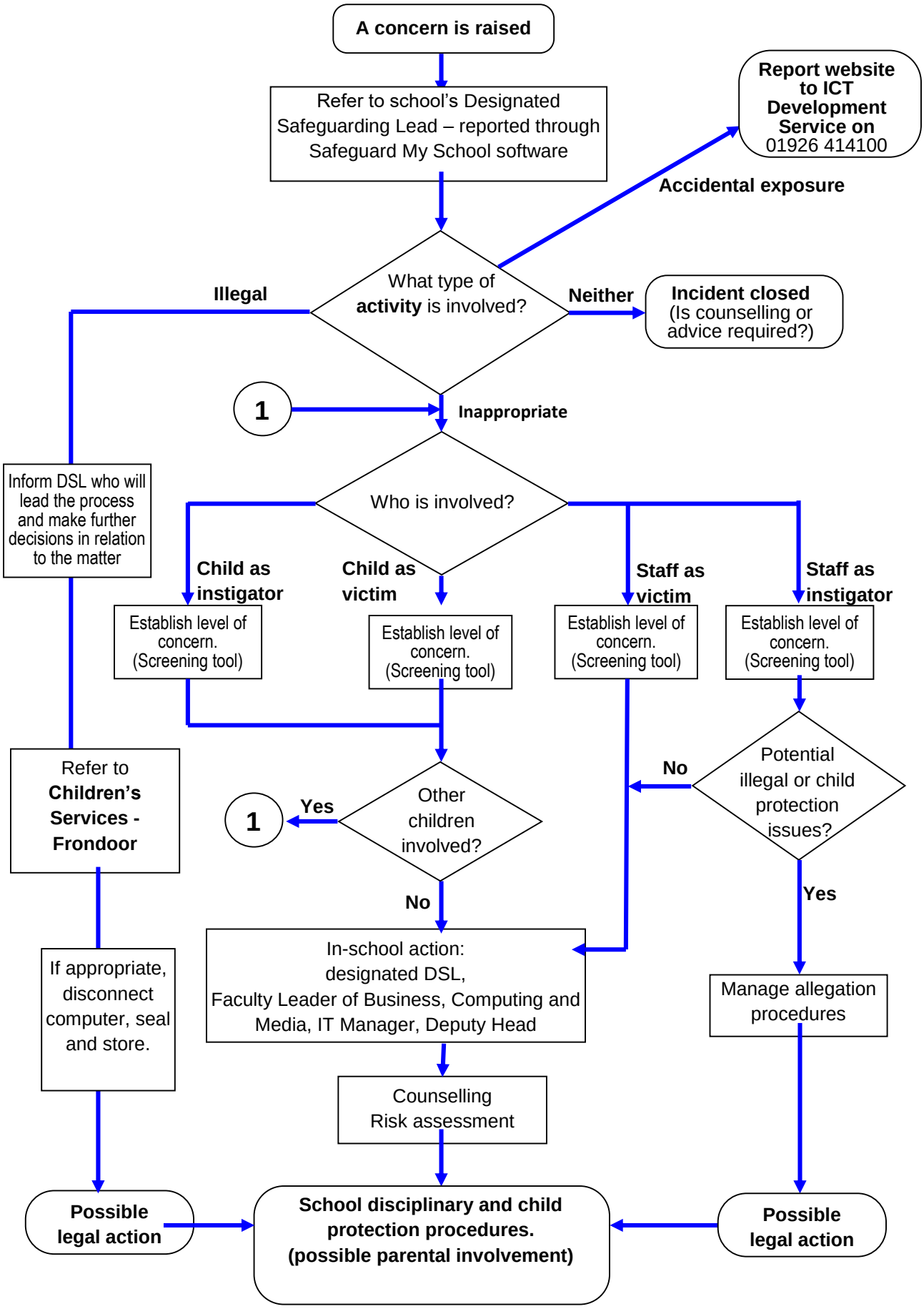
2.3 What are the risks?

- Receiving inappropriate content
- Predation and grooming
- Requests for personal information
- Bullying and threats
- Publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Publishing personal information
- Identity theft
- Hacking and security breaches
- Corruption or misuse of data

2.4 How do we respond?

The flowchart on the next page illustrates the approach to investigating an incident of concern. This diagram should not be used in isolation and instead is used as part of safeguarding practices and procedures.

RESPONSE TO AN INCIDENT OR CONCERN



3.1 Teaching and learning

3.1.1 Why is internet use important?

- The purpose of internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- Students use the internet widely outside school, potentially from a young age and must learn how to evaluate internet information and to take care of their own safety and security whilst online.

3.1.2 How does Internet use benefit education?

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Educational and cultural exchanges between students world-wide;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for students and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with the LA and DfES;
- Education can be provided remotely through the use of online systems;

3.1.3 How can Internet use enhance learning?

- Students will be taught what internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of students.
- Staff should guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.
- Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Access to remote learning when required, available on a range of devices when students cannot access education on school site.

3.1.4 How will students learn how to evaluate Internet content?

- If staff or students discover unsuitable sites, the URL (web address), time, date and content must be reported to the school's IT Support team, Warwickshire ICT Development Service, and where appropriate the school DSL.

- Schools should ensure that the use of internet-derived materials by staff and by students complies with copyright law.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.
- The computing curriculums provides a range of knowledge and understanding regarding how to be safe online and the use of online systems in the modern world.
- The PSHE curriculum ensures emotionally emotive issues online are taught effectively at age appropriate levels.

3.2 Managing Information Services

3.2.1 How will information systems security be maintained?

- The security of the school information systems will be reviewed regularly.
- Virus protection is installed and will be updated regularly.
- The school uses the Warwickshire Broadband with its firewall and filters.
- The school provides an addition level of protection through its use of web-filtering hardware and with the use of screen-monitoring software, for monitoring the use of the internet in the classroom.
- Portable media **may not** be used without specific permission and a virus check.
- Unapproved system utilities and executable files will not be allowed in students' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.

3.2.2 How will e-mail be managed?

- E-mail facilities are available to students, but they can only email those within The Avon Valley School domain.
- Students must immediately tell a teacher if they receive an offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Use of words included in the screen-monitoring software's 'banned' list will be detected and logged.
- E-mail sent to external organisations by staff should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters or spam is not permitted.

3.2.3 How will published content be managed?

- The contact details on the published content should be the school address, e-mail and telephone number. Staff or students' personal information will not be published.
- Email addresses should be published carefully, to avoid spam harvesting.
- The school's Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The published content should comply with the law and guidelines for publications (including respect for intellectual property rights and copyright).

3.2.4 Can staff and students' images or work be published?

- A student's work can only be published with the permission of the student and parents.

3.2.5 How will social networking and personal publishing be managed?

- Social networking sites and newsgroups will be blocked.
- Students are advised never to give out personal details of any kind which may identify them or their location. Examples would include their real name, address, mobile or landline phone numbers, school, social media IDs, email addresses, names of friends, specific interests and clubs, etc.
- Students should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name, school or shopping centre.
- Teachers' **official** blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for students on a personal basis.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Students should be advised not to publish specific and detailed private thoughts.
- Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

3.2.6 How will filtering be managed?

- The school has a procedure in place to ensure filtering systems are as effective as possible.
- If staff or students access unsuitable sites, the URL, time and date must be reported to the school DSL.
- AVS will manage the configuration of the filtering.
- The Faculty Leader with responsibility for ICT will ensure that regular checks are made to check that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported to appropriate agencies such as UK Safer Internet Centre and CEOP.

3.2.7 How will videoconferencing be managed?

The equipment and network

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- External IP addresses should not be made available to other sites.
- Videoconferencing contact information should not be put on the school web site.
- The equipment must be secure and if necessary locked away when not in use.
- School videoconferencing equipment should not be taken off school premises without permission. Use over the non-educational network cannot be monitored or controlled.

Users

- Students should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing should be supervised appropriately for the students' age.

- Responsibility for the use of the videoconferencing equipment outside school time must be established with care.
- Only key administrators should be given access to the videoconferencing system web or other remote control page available on larger systems.
- Unique log on and password details for the educational videoconferencing services should only be issued to authorised members of staff and kept secure.

Content

- When recording a lesson 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.
- If third-party materials are to be included, check that recording is acceptable to avoid infringing the owners' Intellectual Property Rights (IPR).
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- 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.

3.2.8 The management of emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones are banned within the school building for personal use. They may be used to access the Google G Suite for Education platform, but only if requested by a teacher as part of the lesson. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with students is required.
- Staff and student online conversation via email or google classroom is for professional conversations and monitored through IT management.

3.2.9 How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the General Data Protection Regulation (GDPR)
- The Information Commissioner's Office provides relevant information: http://www.ico.org.uk/

3.3 Policy Decisions

3.3.1 How will internet access be authorised?

- The school will maintain a current record of all staff and students who are denied internet access.
- Students must use the internet responsibly and appreciate that their use is monitored through monitoring software.

3.3.2 How will risks be assessed?

- In common with other media such as magazines, books and video, some material available via the internet is unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material

will never appear on a school computer. Neither the school nor WCC can accept liability for the material accessed, or any consequences of internet access.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Head Teacher will ensure that the online safety Policy is implemented and compliant, with the policy monitored.

3.3.3 How will online safety complaints be handled?

- Complaints regarding internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the Head Teacher who should use the agreed WCC procedures.
- Students and parents will be informed of the complaints procedure.
- Parents and students must work in partnership with staff to resolve issues.
- Sanctions within the school discipline policy include:

  - interview/counselling by Achievement Leader;
  - informing parents or carers;
  - detentions;
  - removal of internet or computer access for a period of time.

3.3.4 How is the internet used across the community?

- The school will liaise with local organisations to establish a common approach to online safety.
- The school will be sensitive to internet-related issues experienced by students out of school, e.g. social networking sites, and offer appropriate advice.
- Students can report bullying and sexual harassment both on and offline via our dedicated QR code and google form.

3.4 Communications Policy

3.4.1 How will the policy be introduced to students?

- Rules for internet access will be posted in all networked rooms.
- Students will be informed that internet use will be monitored.
- An online safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede internet access.
- A module on responsible internet use will be included in the PSHE and computing curriculums covering both school and home use.

3.4.2 How will the policy be discussed with staff?

- All staff will be given the School online safety Policy and will have its importance explained.
- All staff will receive dedicated CPD on online safety.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff development on the subject of safe and responsible internet use and on the school online safety Policy will be provided as required.

3.4.3 How will parents' support be enlisted?

- Parents' attention will be drawn to the School online safety policy in newsletters and on the school website.
- Internet issues will be handled sensitively to inform parents without alarm.
- A partnership approach with parents will be encouraged. This could include parents' evenings with demonstrations and suggestions for safe home internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents.
- Interested parents will be referred to organisations listed below (*online safety Contacts and References*).

ONLINE SAFETY CONTACTS AND REFERENCES

Warwickshire ICT Development Service Desk

Help with filtering and network security. 01926 414100

National Online Safety

https://nationalonlinesafety.com/

UK Safer Internet Centre

https://saferinternet.org.uk/

Safety in Schools and Schools online safety Policy

http://clusterweb.org.uk/

Child Exploitation & Online Protection Centre

https://www.ceop.police.uk/Safety-Centre/

Virtual Global Taskforce – Report Abuse

http://virtualglobaltaskforce.com/

Think U Know website

https://www.thinkuknow.co.uk/

Internet Watch Foundation

https://www.iwf.org.uk/

Internet Safety Zone

http://www.internetsafetyzone.com/

Kidsmart

https://www.childnet.com/resources/looking-for-kidsmart/

NSPCC

https://www.nspcc.org.uk/

Childline

https://www.childline.org.uk/

NOTES ON THE LEGAL FRAMEWORK

Many young people and indeed some staff use the internet regularly without being aware that some of the activities they take part in are potentially illegal.

The law is developing rapidly and recent changes include:

- The 2003 Sexual Offences Act has introduced new offences of grooming and raised the age for making/distributing indecent images of children to 18.
- Offences regarding racial hatred are covered by the Public Order Act 1986 although a new Racial and Religious Hatred Bill is going through Parliament.

POSSIBLE OFFENCES

Sexual Offences Act 2003

- **Grooming** – Any communication with a child for the purpose of sexually abusing them is legally considered to be grooming and is classified as an offence under the Sexual Offences Act 2003.
- **Making indecent images** – it is an offence to take, make, distribute, show or advertise indecent images of a child under 18. (NB to view an indecent image on your computer means that you have made a digital image.)
- **Causing a child under 16 to watch a sexual act** – to intentionally cause a child to watch someone else taking part in sexual activity, including looking at images such as videos, photos or webcams, for your own gratification.
- **Abuse of positions of trust** - Staff must be aware that it is an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Applies to teaching staff, teaching assistants, support staff, social workers and health professionals.)
- Information about the 2003 Sexual Offences Act can be found at https://www.legislation.gov.uk/ukpga/2003/42/contents

RELEVANT LEGISLATION

- **The Computer Misuse Act 1990** - makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data. The *Rules for Responsible Internet Use* remind users of the ownership of the school computer system.
- **Public Order Act 1986** – offence to possess, publish or disseminate material intended to/likely to incite racial hatred.
- **Communications Act 2003** - There are 2 separate offences under this act:
  a) sending by means of a public electronic communications network, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character.
  b) sending of a false message or persistently making use of a public electronic communications network for the purpose of causing annoyance, inconvenience or anxiety.
- This wording is important because the offence under *a)* is complete when the message has been sent - no need to prove any intent or purpose. It is an offence under *b)* to keep using the network for sending any kind of message irrespective of content if for the purpose of causing annoyance etc.
- **Malicious Communications Act 1988** – offence to send a letter, electronic communication or article which is indecent or grossly offensive, threatening or false information with intent to cause distress or anxiety to the recipient.
- **Copyright, Design and Patents Act 1988** - it is an offence to use unlicensed software or media
- **Protection of Children Act 1978** - The law on images of child abuse is clear. It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom.
- **Obscene Publications Act 1959 and 1964** - defines “obscene” and related offences.
- **Protection from Harassment Act 1997**
- Section 2 - 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.
- Section 4 - 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 fear on each of those occasions.

SEX OFFENCES ACT 2003 – MEMORANDUM OF UNDERSTANDING

Memorandum of Understanding (MOU) Between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) concerning Section 46 Sexual Offences Act 2003.

The aim of this memorandum is to help clarify the position of those professionally involved in the management, operation or use of electronic communications networks and services who may face jeopardy for criminal offences so that they will be re-assured of protection where they are acting to combat the creation and distribution of images of child abuse. This memorandum has been created within the context of child protection, which will always take primacy.

The MOU: www.iwf.org.uk

SUPPORTING THE DEVELOPMENT OF ONLINE SAFETY

4.1 Regulation

The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. In some cases, access within schools must simply be denied. At AVS, chat rooms present immediate dangers and are banned. Fair rules, clarified by discussion and prominently displayed at the point of access will help students make responsible decisions.

Parents will be informed that students will be provided with supervised internet access. Senior staff will take responsibility for regularly checking that filtering and monitoring is appropriate, effective and reasonable, and that technical staff have not taken on themselves the responsibility for educational or disciplinary issues.

4.2 Appropriate strategies

There are no straightforward or totally effective solutions and staff, parents and the students themselves must remain vigilant. The school will take all reasonable precautions to ensure that users access only appropriate material. Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate. The filtering strategy will be matched to the age and curriculum requirements of the Student.

However, due to the international scale and linked nature of internet content, it is impossible to guarantee that unsuitable material will never appear on a school computer.

AVS will ensure that the use of internet-derived materials by staff and by students complies with copyright law, students will be made aware of plagiarism and issues relating to work research being undertaken for coursework. Staff and students will be trained to become critically aware of the materials they read and shown how to validate information before accepting its accuracy. Students will be taught to acknowledge the source of information used and to respect copyright when using material sourced from the internet in their own work.

4.3 Staff and student electronic communications

Staff and students need to understand that the use of the school's network is a privilege which can be removed should reason arise. The school will monitor all network and internet use in order to ensure student safety.

All users should be expected to adhere to the generally accepted rules of network etiquette (netiquette). These include but are not limited to the following:

- Be polite.
- Use appropriate language.
- Do not get abusive in your messages to others.
- Do not reveal the personal address, phone number or other personal details of yourself or other users.
- Do not use the network in such a way that would disrupt the use of the network by other users.
- Illegal activities are strictly forbidden.
- Note that e-mail is not guaranteed to be private.
- System administrators have access to all mail.
- Messages relating to or in support of illegal activities may be reported to the authorities.

4.4 Using new technologies in education

New technologies should be examined for educational benefit and a risk assessment carried out before use in school is allowed. Secondary schools (and certainly their students) are in the forefront of the use of a huge range of new technologies and learning opportunities including:

- Mobile phones with the power of a PC, with internet, Bluetooth connectivity and a camera.
- New learning environments
- Thinking skills as challenged by games environments and simulations
- Internet voice and messaging such as Skype, FaceTime, WhatsApp and interactive whiteboard (IWB) linking.
- Digital story telling involving independence of thought and self-motivation
- Podcasting, broadcasting and recording lessons, pervasive digital video
- Gaming and gambling on online systems
- Some of these technologies may disappear, but some will change our world. What is important is to combine the experimental ability of youth with the wisdom of teachers to develop appropriate, effective and safe uses in teaching and learning.

REVIEW

This policy will be reviewed every year