Empowering all to achieve

Severn Vale School
An Academy

E-Safety Policy

Date of Policy	September 2026
Date of Next Review	September 2027
Staff Responsible	Designated Safeguarding Lead
Reference	Staff shared area/staff development/policies
School/Governor Policy	Governor

Severn Vale School, Quedgeley, Gloucester, GL2 4PR
01452 720458 • svs@sever nvaleschool.com • www.severnvaleschool.com

Ofsted Good rating

Contents

1 Policy Statement 3

1.1 Background 3

1.2 Scope 4

1.3 Purpose 4

2 Mandate 4

2.1 Roles and responsibility 4

2.2 Communicating School policy 4

2.3 Making use of ICT and the internet in School 5

2.4 Learning to evaluate internet content 5

2.5 Managing information systems 6

2.6 Emails 7

(i) School email accounts and appropriate use 7

2.7 Published content and the school website 7

(i) Policy and guidance of safe use of children's photographs and work 8

Using photographs of individual children 8

(ii) Complaints of misuse of photographs or video 9

(iii) Social networking, social media and personal publishing 9

2.8 Mobile Communication Devices (Phones / Tablets etc) 10

(i) Mobile phone or personal device guidance for staff 10

2.9 Cyberbullying 10

2.10 Managing emerging technologies 11

2.11 Protecting personal data 11

Student Code of Conduct and Acceptable Use Policy (AUP) for ICT 13

1 Policy Statement

1.1 Background

The school recognises that ICT and the internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence.

Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

Severn Vale School continues to encourage and to educate its students in making the most of the opportunities provided by new technologies (including the internet, 'smart' mobile phones, personal portable digital devices).

However, the School acknowledges that there are associated risks to the well-being of children which may include;

Conduct: *Children need to be aware of the impact that their online activity can have on both themselves and other people, and the digital footprint that they create on the internet. It is easy for children to feel anonymous online and it's important that children are aware of who is able to view, and potentially share, the information that they may have posted. When using the internet, it's important children keep personal information safe and not share it with strangers.*

Content: *Some online content is not suitable for children and may be hurtful or harmful. This is true for content accessed and viewed via social networks, online games, blogs and websites. It's important for children to consider the reliability of online material and be aware that it might not be true or written with a bias. Children may need support as they begin to assess content in this way. There can be legal consequences for using or downloading copyrighted content, without seeking the author's permission.*

Contact: *It is important for children to realise that new friends made online may not be who they say they are and that once a friend is added to an online account, they may be sharing your personal information with them. Regularly reviewing friends lists and removing unwanted contacts is a useful step. Privacy settings online may also allow you to customise the information that each friend is able to access.*
If a parent has concerns that your child is, or has been, the subject of inappropriate sexual contact or approach by another person, parents or children can report it to the police via the Child Exploitation and Online Protection Centre(www.ceop.police.uk) and to the school's Safeguarding Team (safeguarding@severnvaleschool.com). If a child is the victim of cyberbullying, this can also be reported online and offline. The school advises that parents reinforce with their child the importance of telling a trusted adult straight away if someone is bullying them or making them feel uncomfortable, or if one of their friends is being bullied online.

Commercialism: *Young people's privacy and enjoyment online can sometimes be affected by advertising and marketing schemes, which can also mean inadvertently spending money online, for example within applications. Children should be taught and advised to keep their personal information private, learn how to block both pop ups and spam emails, turn off in-app purchasing on devices where possible, and use a family email address when filling in online forms.*

(Source: www.saferinternet.org.uk 2021)

The safeguarding of these dangers are tackled in many ways, for example through use of online resources, through both its Computer Science and Futures (PSHE) curriculums, together with guidance on adjusting behaviour to reduce risks including the safe use of electronic devices and the internet. Students are encouraged to build resilience, to protect themselves and their peers, and educated with information about who they should turn to for help and to report concerns.

Severn Vale School recognises the dangers posed by the Internet and, consequently, its ICT system is monitored and managed in ways, which are designed to filter, block and inhibit abuses and to safeguard students in line with government guidance.

As technology and young people's online usage continually evolves and changes the School always strive to make parents and staff aware of relevant guidance and advice, as well as highlight particular risks that stem from safeguarding issues the school encounters and are linked, for example to students use of new Apps or platforms.

1.2 Scope

E-safety covers the internet but it also covers mobile phones/devices, iPads and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of e-safety falls under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential.

1.3 Purpose

This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility.

Cyber-bullying by students will be treated as seriously as any other type of bullying and will be managed through our anti-bullying policy and procedures.

2 Mandate

2.1 Roles and responsibility

The Head and Governors will ensure that the E-safety policy is implemented and compliance with the policy monitored but the day-to-day management of E-safety in the school is the responsibility of the Designated Safeguarding Lead. He/she will work closely with the Head of Futures and senior pastoral and academic staff in this regard.

2.2 Communicating School policy

All staff are provided with a copy of the E-safety policy and this policy is available on the school website for parents, staff, and students to access when and as they wish. Extracts will also be published in the student Handbook. Rules relating to the School Code of Conduct when online, and E-safety guidelines, are displayed around the school. E-safety is integrated into the curriculum in any circumstance where the internet or technology are being used, as well as being specifically addressed in the Futures curriculum. On joining the school, new students are required to agree to

the Student Code of Conduct and Acceptable Use Policy (AUP) for ICT and staff are provided with a Staff Code of Conduct and AUP which they are expected to adhere to.

2.3 Making use of ICT and the internet in School

Using ICT and the internet in school brings many benefits to students, staff and parents. The internet is used in school to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

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 or device connected to the school network. The school cannot accept liability for the material accessed, or any consequences of internet access.

Expectations of use of school computers apply to staff and students both in and out of lessons.

Filtering and Monitoring: Severn Vale School recognises the dangers posed by the Internet. Our school network is monitored by our ICT network manager and access to the Internet is filtered to limit the content that children (and staff) can access from the school computers. Many entertainment and social websites are blocked to keep pupils focused in class and for their safety. Other unsuitable websites are also blocked. In addition, Computer Science teachers use classroom monitoring software to ensure pupils are focused on their work and not distracted by the Internet. The DSL conducts an annual check of the filtering and monitoring system, to ensure inappropriate or illicit online content is blocked accordingly. This is recorded via the school OPSAFE committee meetings and the Governing body is informed.

As technology and young people's online usage continually evolves and changes the School always strive to make parents and staff aware of relevant guidance and advice, as well as highlight particular risks that stem from safeguarding issues the school encounters and are linked, for example to students use of new Apps or platforms. The school has a dedicated Online Safety page on its website to inform and signpost students and parents.

Staff Online Safety

The School recognise the recommendations made in KCSIE 2024 that staff awareness of online risks and knowledge of how to counter these and advise young people is of great importance.

Staff are briefed annually by the Safeguarding Team on online risks and dangers and receive regular updates/advice from the Safeguarding Team as well as the Subject Leader for Computer Science. More bespoke training is offered for staff on certain areas, dependent on identified needs. Staff are also made aware of the filtering and monitoring systems in place.

2.4 Learning to evaluate internet content

With so much information available online it is important that students learn how to evaluate internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Students will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate;
- to acknowledge the source of information used and to respect copyright. The school will take any intentional acts of plagiary very seriously.

If staff or students discover unsuitable sites then the URL, time, date and content must be reported to the IT Department. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies via the IT Department or a member of the Senior Management Team. Regular checks will take place to ensure that filtering services are working effectively.

2.5 Managing information systems

The school is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the school information systems and users will be reviewed regularly by the IT Support team and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- Making sure that unapproved software is not downloaded to any school computers. Files held on the school network will be regularly checked for viruses;
- The use of user logins and passwords to access the school network will be enforced;
- Portable media containing school data or programmes will not be taken off-site without specific permission from the School Business Manager.

My Concern Platform

Severn Vale school uses My Concern.

My Concern is a digital web-based platform, developed by child protection experts, with backgrounds in social care, education and policing. My Concern allows staff responsible for the protection of children, young people at risk to easily manage and record all safeguarding and wellbeing concerns in one central location.

Oversight of My Concern is the primary responsibility of the DSL and Deputy DSL, however other key pastoral and Administrative staff also have access to the platform and can input information, as well as keep and update student chronologies.

The platform has multiple layers of security and staff user access is determined by the DSL.

Staff with access to sensitive data on My Concern are required to read and sign a separate Acceptable Use agreement in line with its use.

For more information on data protection in school please refer to our Data Protection policy, which can be accessed on the school's website. More information on protecting personal data can be found in section 11 of this policy.

2.6 Emails

The school uses email internally for staff and students, and externally for contacting parents, and is an essential part of school communication.

Access in school to external personal email accounts may be blocked. The school has the right to monitor emails and their contents but will only do so if there is suspicion of inappropriate use.

(i) School email accounts and appropriate use

Staff should be aware of the following when using email in school:

- Staff should only use official school email accounts for school-related matters, contact with other professionals for work purposes and to communicate with students, parents or carers. Personal email accounts should not be used to contact any of these people.
- Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.
- For any awkward, sensitive, easily misinterpreted situations or anything that may have legal repercussions, staff should have the content of their email checked carefully by their line manager or a senior member of staff.
- Staff must tell their manager or a member of the Senior Management Team if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.
- The forwarding of chain messages is not permitted in school.
- The ICT Acceptable Use policy / agreement gives further information. Staff are required to read this annually and sign to say that they have done so.

Students should be aware of the following when using email in school, and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:

- All students are provided with a school email account and students may only use approved email accounts on the school system.
- Students are warned not to reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission. Excessive social emailing can interfere with learning and in these cases will be restricted.
- Students should immediately inform a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.

2.7 Published content and the school website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students and staff for keeping up-to-date with school news and events, celebrating whole-school achievements, personal achievements and promoting school projects.

The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community,

copyrights and privacy policies. No personal information on staff or students will be published. For information on the school policy on children's photographs on the school website please refer to section 2.7(i) (below) of this policy.

A team of staff, under the leadership of the Headteacher are responsible for publishing and maintaining the content of the school website. The website will comply with the school's guidelines for publications including respect for intellectual property rights and copyright. Staff and students will be made aware of copyright in respect of material taken from the internet.

Students should not publish anything on the internet involving the school unless permission has been granted by the Headteacher.

(i) Policy and guidance of safe use of children's photographs and work

Colour photographs and students work bring our school to life, showcase our students' talents, and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under the General Data Protection Regulation images of students and staff will not be displayed in public, either in print or online, without consent.

Using photographs of individual children

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.

It is important that published images do not identify students or put them at risk of being identified. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission, with the exception of parents taking photographs or videos at school events involving their son or daughter for personal use only (as defined by the Information Commissioner's Office ICO).

The school follows general rules on the use of photographs of individual children:

- Consent from parents will cover the use of images in:
    - all school publications
    - on the school website
    - in videos made by the school or in class for school projects.
- Electronic and paper images will be stored securely.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that students are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the students (i.e. a student in a swimming pool, rather than standing by the side in a swimsuit).
- For public documents, including in newspapers, full names will not be published alongside images of the child without the written permission from parents. Groups may be referred to collectively by year group or form name.

- Events recorded by family members of the students such as School drama productions or sports events must be used for personal use only.
- Students are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the students.

(ii) Complaints of misuse of photographs or video

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our complaints policy for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with school policy.

(iii) Social networking, social media and personal publishing

Personal publishing tools include blogs, wikis, social networking sites, bullet-in boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online. The school will normally block/filter access to social networking sites via the school network.

Social media sites have many benefits, however both staff and students should be aware of how they present themselves online. Students are taught through the ICT curriculum and PSHE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

- Students are educated on the dangers of social networking sites and how to use them in safe and productive ways. Students are advised never to give out personal details of any kind which may identify them or their location. They are all made fully aware of the School's code of conduct regarding the use of ICT and technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official school blogs created by staff or students/year groups/school clubs as part of the school curriculum will be moderated by a member of staff.
- Students and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and students to remember that they are representing the School at all times and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction and guidance is provided through the ICT Staff code of conduct and AUP.

2.8 Mobile Communication Devices (Phones / Tablets etc)

Mobile phone and other personal devices are now an important part of everyone's life and have considerable value, particularly in relation to individual safety. Whilst these devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are that:

- they can make students and staff more vulnerable to cyberbullying;
- they can be used to access inappropriate internet material;
- they can be a distraction in the classroom;
- they are valuable items that could be stolen, damaged, or lost;
- they can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The DfE has made clear its expectation for schools to implement a policy whereby pupils do not have access to their mobile phone throughout the school day including during lessons, the time between lessons, breaktimes and lunchtime. In line with this guidance Severn Vale enforces a strict mobile phone policy as detailed within our Behaviour policy) which requires any student who chooses to bring a phone to school to place it into a lockable pouch on entry to the school. This will ensure that mobile devices do not negatively impact learning, safety, or conduct.

(i) Mobile phone or personal device guidance for staff

- Staff are expected to have read and be aware of the school's Social Networking Whole School Guidance for Teachers
- Staff should only use school equipment if photos or videos are being taken as part of the curriculum or in a professional capacity.
- Staff must not use their own personal devices to text or phone students either in or out of school time.
- Any breach of school policy may result in disciplinary action against that member of staff.
- Staff are advised not to contact parents on their personal devices.
- In line with the new DFE guidance the school expects staff to lead by example regards use of mobile devices. Where possible staff should avoid open use of mobile phones for personal reasons (including use of social media), when in the vicinity of students.

Further Info:
www.saferinternet.org.uk
www.ceop.police.uk/Safety-Centre/
www.childnet.com/teachers-and-professionals
www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/teaching-resources

2.9 Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the school. Information about specific strategies to prevent and tackle bullying are set out in the school's Behaviour policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

If an allegation of bullying does come up, the school will:

- take it seriously;
- act as quickly as possible to establish the facts. It may be necessary to examine School systems and logs or contact the service provider in order to identify the bully;
- record and report the incident;
- provide support and reassurance to the victim;
- make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. They may have their internet access suspended in School.

2.10 Managing emerging technologies

Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

2.11 Protecting personal data

The school believes that protecting the privacy of our staff and students and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from students, parents, and staff and processes it in order to support teaching and learning, monitor and report on student and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. Results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the well-being and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

In line with General Data Protection Regulations, and following principles of good practice when processing data, the school will:

- ensure that data is fairly and lawfully processed;
- process data only for limited purposes;
- ensure that all data processed is adequate, relevant and not excessive;
- ensure that data processed is accurate;
- not keep data longer than is necessary;
- process the data in accordance with the data subject's rights;

- ensure that data is secure;
- ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the school's safeguards relating to data protection please refer to the school's Data Protection Policy and Privacy Statements.

Appendix 1:

Student Code of Conduct and Acceptable Use Policy (AUP) for ICT

You are responsible for good behaviour when using IT Equipment in school and accessing the internet, just as you are in all other aspects of life at school. This includes your own mobile devices with internet access. Communications on the network are often public in nature. The code of conduct applies at all times, in and out of school hours, when using school resources and equipment.

Network and internet access is provided for students to conduct research and communicate with others. Independent access to these services is provided to those who agree to act in a considerate and responsible manner and receive parental permission. Access is a privilege, not a right. Access entails responsibility.

Individual users are responsible for their behaviour and communications over the network. It is presumed that you will comply with this code and will follow the agreements you have signed.

User areas on the school network will be monitored, and staff may review your files and communications to maintain system integrity.

During lessons, teachers will guide students towards appropriate materials. Outside lesson-time, you must only access sites which are appropriate for use in School.

The following are not permitted:

- Using another user's identity
- Sending or displaying offensive messages or pictures
- Using or displaying obscene language
- Violating copyright laws
- Intentionally wasting limited resources
- Employing the network for commercial purposes
- Using chat or games sites
- Downloading program files/copyright material (e.g. MP3 files)
- Using portable computers in lessons without the express permission of the teacher.
- Using mobile phones in school.

Students should not publish anything on the internet involving the school unless permission has been granted by the appropriate SLT line manager.

Further guidance for students is published in the Student Handbook in the section headed: Computer Use by Students.

Failure to comply with the code will result in loss of access and further disciplinary action may be taken if appropriate. If applicable, external agencies may be involved.

Related Documents:

- Safeguarding & Child Protection Policy
- Behaviour Policy
- Student Handbook
- Code of Conduct and Whistleblowing Policy
- Acceptable Use Policy (AUP) for ICT
- Code of Conduct for ICT Systems Administrators
- Data Protection Policy

Appendix 2:

Social Networking Guidance

Social networking offers a world of possibilities to teaching. Many staff and young people in schools are already users of sites such as Facebook and Twitter However, it is essential to ensure that staff keep themselves and young people safe online and, as teachers, staff have a key role to play in actively promoting these safety messages.

For the link to the Social Networking guidance document issued to staff please follow this link.

Appendix 3:

Online Safety Web page

The school offers advice and guidance to students and parents via its Online Safety page of the school website.

https://www.severnvaleschool.com/school/online-safety