SELWOOD ACADEMY
ANGLICAN/METHODIST FOUNDATION SCHOOL

E-Safety Policy
2024

"Let your light shine before others"
Matthew 5 v 16

The following policy is reflective of our deeply held Christian Vision and Values .

Vision

We are committed to creating a safe, happy and enriching environment where we all aspire to thrive, achieve and celebrate success together.
Our aim is to promote the dignity and well-being of every child and staff member and ensure they flourish in the course of their journey with us.

Values

Our core Christian values of Hope, Wisdom , Community and Joy underpin all that we strive to achieve to enable our 'light to shine before others' **Matthew 5 v 16**

Contents

Responsible Committee: **Resources Committee**
Date Last Reviewed: **October 2024**
Due to be Reviewed: **October 2027**

- Education and training – Staff
- Training – Trustees
- Technical – infrastructure/equipment, filtering and monitoring
- Curriculum
- Use of digital and video images
- Data protection
- Communications
- Unsuitable/inappropriate activities
- Responding to incidents of misuse

Appendices:

- Pupil/Parent/Carer Acceptable Use Policy Agreement
- Staff and Volunteers Acceptable Use Policy Agreement
- Staff Unfiltered Internet Access Acceptable Usage Policy

Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. These technologies can stimulate discussion, promote creativity and enhance effective learning.

Children and young people should have an entitlement to safe internet access at all times and the Selwood Academy E-Safety policy will help to promote and ensure safe and appropriate use of the internet and related technologies, by involving all stakeholders in our children's education.

The internet and other digital technologies can put young people at risk within and outside the school and it is the duty of care of all who work within the school as well as parents and the wider school community to protect our children from these dangers. 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 young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with our other policies (eg relationship, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' 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.

We must as an Academy demonstrate that we have provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development / Monitoring / Review

The implementation of this E-Safety Policy will be monitored by the Trustees' Resources Committee. The Trustees Resources Committee will discuss safeguarding as an agenda item at each meeting, which will include e-safety. The E-Safety Policy will be reviewed biennial, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be October 2027. Should serious e-safety incidents take place, the following Academy staff should be informed:

Mr D Jeffries (Headteacher)

Responsible Committee: **Resources Committee**
Date Last Reviewed: **October 2024**
Due to be Reviewed: **October 2027**

Mrs Batchelor (Designated Safeguarding Lead)
Mr Finlay (Curriculum E-Safety Officer)
Miss Singer (Business E-Safety Officer)
Other Academy Staff or external agencies will be informed as necessary.

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, parents/carers, Trustees, volunteers, visitors, community users) who have access to and are users of Selwood Academy ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Head-teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but are linked to membership of the school.

The Academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Trustees:

Trustees are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Trustees receiving information about e-safety incidents and monitoring reports. As of October 2024, the Trustee responsible for safeguarding will also be responsible for e-safety. The role involves:

- Meetings with the Curriculum and Business E-Safety Officers
- Monitoring of e-safety and filtering logs and incident reports
- Monitoring of filtering/change control logs
- Reporting to relevant Trustees committee/meeting

Headteacher and Senior Leaders:

The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Curriculum and Business Officers

- The Headteacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher ensures that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive monitoring reports from the E-Safety Officers.
- The Headteacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart for dealing with e-safety incidents – included in a later section – “Responding to incidents of misuse” and relevant HR/disciplinary procedures)

E-Safety Officers:

- lead e-safety within the school
- take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provide training and advice for staff
- liaise with school ICT technical staff
- receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments,
- meet with E-Safety Trustee to discuss current issues, review incident logs and filtering / change control logs – these meetings may be electronic in nature.
- attend relevant meeting/committee of Trustees
- Report to Senior Leadership Team

Apollo Technology & Network Provider:

Apollo Technology is responsible for ensuring:

- That the Academy's ICT infrastructure is secure and is not open to misuse or malicious attack
- That the Academy meets the e-safety technical requirements in the Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- That users may only access the school's networks through a properly enforced password protection policy.
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- That the use of the network/ remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the E-Safety Co-ordinator
- That monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff:

Are responsible for ensuring that

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood and signed the Academy's Staff Acceptable Use Policy/Agreement (AUP)
- They report any suspected misuse or problem to the E-Safety Co-ordinator for investigation/action/sanction
- Teachers and support staff do not communicate with pupils on personal devices.
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Pupils understand and follow the school e-safety and acceptable use policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended school activities

- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices

Designated Safeguarding Lead:

Should be trained in e-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
- Cyber-bullying

The designated E-Safety officers have the following powers in respect of child protection.

The E Safety officer is allowed to access sites or workspaces owned by students where a significant child safety risk is posed. In all cases parents/guardians should be contacted but if permission for access is refused then the school still retains the right to this access if the Designated Safeguarding Lead, the E-Safety officer and the Headteacher/Senior officer present in school on that day agree.

Trustees' Resources Committee

Trustees' will assist the E-Safety Officers with:

- The production/review/monitoring of the school e-safety policy/documents.
- The assistance in monitoring information services to parents.

Pupils:

- Are responsible for using the Academy's ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- 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, digital cameras and 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 e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers:

Parents/Carers 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 carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings,

newsletters, letters, website and information about national/local e-safety campaigns/literature. Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil / Parent Acceptable Use Policy
- Accessing the school website/ in accordance with the relevant Pupil / Parent Acceptable Use Policy.
    - Upholding the principles of the relevant Pupil/Parent Acceptable Use Policy in relation to their own use of the internet and social media, when that use is related in any way to the school, or to any employees, pupils or Trustees associated with it.

Community Users:

Community Users who access school ICT systems / website as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided. This will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages will be reinforced as part of a planned programme of assemblies.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all rooms with pupils ICT access.
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents/carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- Parents evenings

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of e-safety training will be made available to staff.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies. This will be carried out through the induction programme that new staff receive. In addition to this the school offers this training to all trainee teachers and assistants who work at the school, whether temporary or permanent.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The E-Safety Officers will provide advice/guidance/training as required to individuals as required.

Training – Trustees

Trustees should take part in e-safety training/awareness sessions, with particular importance for those who are members of any subcommittee/group involved in ICT/e-safety/health and safety/child protection. T

- Participation in school training/information sessions for staff or parents

Technical – infrastructure/equipment, filtering and monitoring

The Academy will be responsible for ensuring that the infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- Academy ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements.
- There will be regular reviews and audits of the safety and security of the Academy ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted where possible
- All users will have clearly defined access rights to school ICT systems through group policy. Users can be made aware of their own group policy access rights at any time by contacting the E-Safety Business Officer, although any requested changes to these access rights is solely at the discretion of the Headteacher. Any changes must comply with this e safety policy and the AUP of the requesting individual.
- All users will be provided with a username and password by the ICT technical staff who will keep an up to date record of users and their usernames.
- The “master/administrator” passwords for the school ICT system, used by the Network/ICT technical staff (or other person) must also be available to the Head teacher or other nominated senior leader and kept in a secure place (eg school safe)
- Users will be made responsible for the security of their username and password, 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.
- The Academy maintains and supports the managed filtering service provided by Smoothwall and supported by Apollo Technology.
- Any filtering issues should be reported immediately to the network provider via Apollo Technology or Director of Business and Finance in their absence.

- Requests from staff for sites to be removed from the filtered list will be considered by the Headteacher If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Officers.
- Academy ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- An appropriate system is in place for users to report any actual/potential e-safety incident to the ICT Technician (or other relevant person).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system. All temporary staff must sign the staff AUP and be made aware of this e safety policy
- An agreed policy is in place through the AUP's regarding the downloading of executable files by users
- An agreed policy is in place through the AUP's that forbids staff from installing programmes on school workstations/portable devices. If they need to instal a programme they can contact Apollo Technology.
- An agreed policy is in place through the AUP's regarding the use of removable media (eg memory sticks/CDs/DVDs) by users on school workstations/portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- in lessons where internet use is pre-planned, it is best practice that 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.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils 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 carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular 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 school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils 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.
- Pupils full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or marketing and other materials.
- Student's work can only be published with the permission of the pupil.

General Data Protection Regulation

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 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.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
    - Ensure that no personal data is displayed on the Interactive white board or other display.
- Always lock the screen when they are not at their workstation/computer.
- Transfer data using encryption and secure password protected devices.
- The use of portable computer systems, USB sticks or any other removable media is permitted, however this must be within the guidelines of this policy and that of GDPR. All staff are asked to liaise with Business Manager to clarify use.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to lessons	*							*
Use of mobile phones in lessons				*			*	
Use of mobile phones in social time	*							*
Taking photos on personal mobile phones or other camera devices				*				*
Use of mobile devices for school business	*					*		
Use of personal email addresses in school, or on school network		*						*
Use of school email for personal emails				*				*
Use of chat facilities for school business	*						*	
Use of instant messaging for school business	*						*	
Use of social networking sites for school business			*					*
Use of blogs for school business			*			*		

When using communication technologies, the Academy considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems.
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the Headteacher – 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 pupils or parents/carers (email, chat, 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.
- Pupils 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 write 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.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
All users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**child sexual abuse images**					*
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					*
	adult material that potentially breaches the Obscene Publications Act in the UK					*
	criminally racist material in UK					*

	pornography				*	
	promotion of any kind of discrimination				*	
	promotion of racial or religious hatred				*	
	threatening behaviour, including promotion of physical violence or mental harm				*	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				*	
Using school systems to run a private business					*	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the network provider and / or the school					*	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					*	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					*	

Creating or propagating computer viruses or other harmful files				*	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet			*		
On-line gaming (educational)		*			
On-line gaming (non educational)			*		
On-line gambling				*	
On-line shopping / commerce			*		
File sharing (using p2p networks such as U Torrent)				*	
Use of social networking sites			*		
Use of video broadcasting eg Youtube		*			

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Equally the school will follow the policies laid out in the Child Protection documentation and will inform the necessary member of staff immediately to ensure the safeguarding of our young people.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a “clean” designated computer.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students/Pupils **Actions**

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	*	*	*	*	*	*	*		*
Unauthorised use of non-educational sites during lessons	*	*			*	*			
Unauthorised use of mobile phone / digital camera / other handheld device	*	*				*			*
Unauthorised use of social networking / instant messaging / personal email	*	*			*	*		*	*
Unauthorised downloading or uploading of files	*	*			*	*			*
Allowing others to access school network by sharing username and passwords	*	*			*			*	
Attempting to access or accessing the school	*	*			*				*

Responsible Committee: **Resources Committee**
Date Last Reviewed: **October 2024**
Due to be Reviewed: **October 2027**

network, using another student's / pupil's account									
Attempting to access or accessing the school network, using the account of a member of staff	*	*	*		*	*	*	*	*
Corrupting or destroying the data of other users	*	*			*	*	*	*	*
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	*	*			*	*	*	*	*
Continued infringements of the above, following previous warnings or sanctions	*	*	*		*	*	*	*	*
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	*	*	*		*	*	*	*	*
Using proxy sites or other means to subvert the school's filtering system	*	*			*	*	*	*	*
Accidentally accessing offensive or pornographic material and failing to report the incident	*	*			*	*		*	
Deliberately accessing or trying to access offensive or pornographic material	*	*	*		*	*	*	*	*
Receipt or transmission of material that infringes the copyright of	*	*	*		*	*	*	*	*

another person or infringes the Data Protection Act									

Staff / Volunteers **Actions**

Incidents:	Refer to line manager	Refer to Head teacher	Refer to HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		*	*	*			*	*
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email during school time.		*				*	*	*
Unauthorised downloading or uploading of files	*				*			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		*				*		
Careless use of personal data eg holding or transferring data in an insecure manner		*			*			
Deliberate actions to breach data protection or	*	*	*		*	*	*	*

network security rules								
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		*	*					*
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	*	*	*					*
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils under the age of 18 or still in full-time education.	*	*	*					*
Actions which could compromise the staff member's professional standing	*	*	*			*	*	*
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	*	*	*			*	*	*
Using proxy sites or other means to subvert the school's filtering system	*	*	*					*
Accidentally accessing offensive or pornographic material and failing to report the incident	*	*	*		*	*		
Deliberately accessing or trying to access offensive or pornographic material	*	*	*		*	*	*	*
Breaching copyright or	*							*

licensing regulations								
Continued infringements of the above, following previous warnings or sanctions	*	*	*		*	*	*	*

Appendices

Can be found on the following pages:

- Pupil/Parent Acceptable Usage Policy
- Staff and Volunteers Acceptable Usage Policy
- Staff Unfiltered Internet Access Acceptable Usage Policy

Pupil/Parent Acceptable Use Policy Agreement
Selwood Academy has a clear policy when allowing pupils to access the schools ICT network.
This document is designed to keep you safe and is split into different sections:

Personal Benefits	Equality	How I treat others	Helping the school	Being a responsible citizen

Personal Benefits

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password securely I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

Equality

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are for educational use and that I will not use the systems for personal use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

How I treat others

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images or video of anyone without their permission.

Helping the school

I recognise that Selwood Academy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my personal hand held / external devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or

software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a device/computer, or store programmes on a computer, nor will I try to alter computer settings.

Being a responsible citizen

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including pictures, music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

When using the internet and social media outside of school, I recognise that:

- I must not post messages about the school or anyone associated with it that are untruthful, unlawful, libellous, harassing, defamatory, abusive, threatening, harmful, obscene, or sexually or racially offensive in any way.
- I must not post or share images of anyone associated with the school without their permission
- I must not impersonate someone else
- I must not post content copied from elsewhere, for which I do not own the copyright.
- I must follow the guidelines I have been taught about safe and appropriate use of the internet and digital and communication technologies

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of very serious or illegal activities, involvement of the police.

By Attending Selwood Academy, you agree to our Home School agreement and therefore the guidance and rules in this policy.

Pupil/Parent Acceptable Use Agreement Form

As a pupil you have read, understood and agree to the rules included in the Acceptable Use Agreement

PUPIL: I have read and understand the above and agree to follow these guidelines when:

- I use Selwood Academy's ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) or for any school activity e.g. mobile phones, cameras etc
- I use my own equipment out of school in a way that is related to me being a member of this school.

PARENT/CARER:

- I agree to support and uphold the principles of this policy in relation to my child.
- I agree to uphold the principles of this policy in relation to my own use of the internet and social media when that use is related to the school, or to any employees, pupils or Trustees associated with it.

Selwood Academy – Acceptable Use Policy – Staff + Volunteers

The aim of this policy is to:

- Allow staff/volunteers access to and use of computer equipment for education purposes according to acceptable procedure
- Protect staff/volunteers and pupils from sources of information and individuals such as would undermine the principle and aims of the school.
- Provide rules which are consistent and in agreement with the General Data Protection Regulation and Misuse of Computers Act
- Provide rules which are consistent with acceptable procedures commonly used on the Internet

The primary purpose of the ICT network and systems are education. Personal use by staff is acceptable (outside of school hours), but use must conform to the AUP at all times.

Do not disclose your password to anyone and ensure that your computer equipment is locked or logged off at all times that you are not present. It is recommended that you change your password on a regular basis. Do not disclose any personal data, including telephone, fax and email information relating to any other adult or pupil at the school.

Use of names and photographs of pupils in internal or external publications (including social networking sites) will require written permission from parents.

Ensure that any private social networking sites (Instagram, facebook etc) that I create, edit or contribute to and any online activity that I engage with inside or outside of school does not compromise my professional role within school. Under no circumstances is any communication to be written in such a way as may be considered untruthful, unlawful, libellous, harassing, defamatory, abusive, threatening, harmful, obscene, or sexually or racially offensive. Photographs taken in a school context are not to be shared on any private social networking sites.

The Academy must use a filtered internet service and therefore some sites may not be available in school. No service however is 100% secure and therefore the following rules must apply:

You must not download or use any materials which are copyright protected. Always seek permission from the owner before using material from the Internet. If you cannot gain permission, do not use the material.

In no circumstances should you view, upload, download or send material which is likely to be unsuitable for children or deemed offensive by colleagues. This applies to but not limited to any material with a violent, dangerous, racist or inappropriate sexual content. Any such infringement could result in disciplinary or police action.

When communicating using the ICT network and systems for any school business you must use the approved school email service. Under no circumstances is any communication to be written in such a way as may be considered abusive, defamatory or libellous. Any such communication will be deemed to be the personal views of the individual, who will also accept all liability. Special care must be taken to ensure that written statements cannot be construed out of context and lead to possible legal action.

I will not download any software or resources from the internet that could compromise the ICT network and systems or use any software which is not adequately licensed.

I understand that the school monitors all computer related activity including internet access through internal mechanisms including automatic monitoring via specific computer software and will report any infringement or breach of the Acceptable use policy (AUP).

I do not store or transport personal data on any portable computer system, USB stick or any other removable media.

I will only connect a computer, laptop or other device to the 'Guest' ICT network and systems that is provided by the school, I will ensure computer equipment is up-to-date using the schools anti-virus software by regularly connecting equipment to the school network. I will be responsible for the actions of anyone I permit to use the computer equipment provided by the school.

I agree and accept that any computer equipment loaned to me by the school is provided solely to support my professional responsibilities. I will notify the school of any significant personal use as defined by HM Customs and Revenue. HM customs and Revenue state: "If the computer is provided solely for business use and any private use is not significant, the computer continues to be exempt from a benefit charge".

I will not transfer, copy or make public any software that I am given to aid my professional duties by the school or any copyrighted materials belonging to any third parties.

I will not intentionally interfere with the normal operation of the internet, including the propagation of viruses. I will inform the ICT department if I need to transfer large files across the network that may interfere with the normal running of the network.

Responsible Committee: **Resources Committee**
Date Last Reviewed: **October 2024**
Due to be Reviewed: **October 2027**

I will not use the network, internet or school ICT equipment for any action that is deemed inappropriate by the Head Teacher.

I will report any breach of the above Acceptable Use Policy to my line manager. I will ensure that any information I receive regarding children becoming victims of any breach of the student AUP or any incident which compromises there safety online or otherwise is reported to the child protection officer. Equally I will report to a relevant senior leader any incident involving electronic communications whether from a child or adult that compromises my safety.

I confirm that I have read, understood and agreed with the staff Acceptable Use Policy.

Name (Printed): _____

Signed: _____

Date: _____

A copy of this signed acceptable use policy is required to be held on record by the ICT department. This will be stored in your personnel file and is accessible via the Business Manager

The form can also be signed electronically when read using My Concern safeguarding website.

Selwood Academy – Acceptable Use Policy – Staff
Unfiltered Internet Service

By signing this form you accept and fully understand that any breach of this acceptable use policy could result in disciplinary action by the school / police

Access to the Unfiltered Internet Service is available to all staff via their personal network log in.

REMEMBER: Unfiltered Access will display any pop-ups, adverts or images that would otherwise have been filtered – take care when searching online.

REMEMBER – If a pupil contacts you with regards to problems they are experiencing with social networking, you must not try to deal with this yourself using your Unfiltered Access. You MUST report this to the Designated Safeguarding Lead (Carmen Batchelor) or the E Safety Officer (Dave Finlay).

I will ensure that when using Unfiltered Internet Service I do not display materials that are inappropriate through my whiteboard.

Responsible Committee: Resources Committee
Date Last Reviewed: October 2024
Due to be Reviewed: October 2027

I will not download materials that may be harmful to the school network or that breach the staff AUP.

I will ensure that my PC is locked at all times when I am not using it. Failure to do this will result in your machine being altered to auto-lock after a set period of time.

I will not allow students to use my PC at any point for any purpose.

I will at no point use the Unfiltered Internet Service in any way that may bring the school into disrepute or may harm my professional standing.

I will not download and install any software at any point for any reason. I will at all times comply with the Staff AUP for which I will have signed in order to be authorised to use the Unfiltered Internet Service. I will refrain from "streaming" large video files or using streaming audio sites that could slow down the school network.

I am aware that the Unfiltered Internet Service is provided to me solely for the purpose of aiding effective teaching and learning and not for me to use socially.

I must continue to use only the designated email service (@selwood-academy.co.uk). I am not permitted to use hotmail or any other third party email service for any professional communications.

I must always close my browser when I have finished using the unfiltered network and must not allow anyone else to use the service through my connection. Any content browsed is at your liability when logged on as you.

If at any point I see or access material accidentally that I feel is inappropriate I must stop what I am doing and report it immediately to the ICT office.

I confirm that I have read, understood and agreed with the Unfiltered Internet Service Acceptable Use Policy. If at any point I am concerned that an action I may take could breach the AUP in any way Don't Do It. Check It.

Name (Printed): _____

Signed: _____

Date: _____/_____/_____

A copy of this signed acceptable use policy is required by the school and will be stored in your personnel file.

Responsible Committee: Resources Committee
Date Last Reviewed: October 2024
Due to be Reviewed: October 2027