E-Safety Policy

Approved by:	Full Governors	**Date:** October 2023
Last reviewed on:	October 2025	
Next review due by:	October 2026	

Contents

1. The Aims of the Policy

The e-Safety Policy applies to all members of Willow Bank community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of Willow Bank Schools ICT systems and mobile technologies, both in and out of Willow Bank.

The purpose of this Policy is to provide the staff of Willow Bank School appropriate procedures for the protection of safeguarding of children in and out of Willow Bank when interacting with the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people, and adults in danger. Any questions regarding its operation should be addressed to the Headteacher or Deputy Headteacher.

E-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, Twitter, mobile phones and other electronic communications technologies, both in and out of Willow Bank. It includes education for all members of Willow Bank community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

Willow Bank School must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating students and staff about responsible use. Willow Bank School must be aware that children and staff cannot be completely prevented from being exposed to risks both on and offline.

Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good e-Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours' compatible with their role.

Breaches of an e-Safety policy can and have led to civil, disciplinary, and criminal action being taken against staff, pupils, and members of the wider community. It is crucial that all settings are aware of the offline consequences that online actions can have. Schools must be aware of their legal obligations to safeguard and protect children on and offline and the accountability of these decisions will sit with the Head Teacher and the Governing body.

The e-Safety policy for Willow Bank School is essential in setting out how Willow Bank plans to develop and establish its e-Safety approach and to identify core principles which all members of Willow Bank community need to be aware of and understand.

Any concerns please refer to Mrs. N Laughton or members of the SLT.
Designated person for Safeguarding: Mr J McKune
Governor for Safeguarding: Mrs M Neale

2. Policy Governance

Development, Monitoring and Review of this Policy

This e-safety policy has been reviewed by a working group / made up of:

Position	Name(s)
Willow Bank School E-Safety Coordinator	Mr. McKune
School Safeguarding Officer (DSL)	Mr. McKune
Headteacher	Mrs. Laughton
Governor	Mrs. Neale

Consultation with Willow Bank School has taken place through the following:

Forum	Date (if applicable)
Staff meetings / Briefing	Reminder to staff of 'e- safety' concerns
Willow Bank/ Student / Pupil Council	Discussion on dangers of Internet Use – Cyber Bullying.
Willow Bank School / website	Intranet - Newsletter

3. Schedule for Review

This e-safety policy was approved by the *Governing Body*	October 2025
The implementation of this e-safety policy will be monitored by:	The Senior Leadership Team
Monitoring will take place at regular intervals:	Yearly
The Governing body will receive a report on the implementation of the e-safety policy generated by Jon McKune at regular intervals:	At least once a year
The E-Safety Policy will be reviewed annually, 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 2026
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	LA ICT Manager LA Safeguarding Officer (LADO) Police

4. Scope of the Policy

This policy applies to all members of Willow Bank community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of Willow Bank ICT systems and mobile technologies including Twitter both in and out of Willow Bank.

5. Role and Responsibilities

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

Governors

- Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Headteacher and Senior Leaders – Nicola Laughton, Eve Bainbridge, and Jon McKune

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of Willow Bank community
- The Headteacher and another member of the Senior Leadership Team/Senior Management Team 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. This team member will be Mr J McKune (DSL).

E-safety Coordinator Officer – Jon McKune

- Leads the e-safety committee and/or cross- initiative on e-safety
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing Willow Bank e-safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Reports regularly to Headteacher and Governors

Network Manager / Technical Staff

St Helens Council will be responsible for ensuring:

- That Willow Bank's ICT infrastructure is secure and is not open to misuse or malicious attack
- That Willow Bank meets the e-safety technical requirements outlined in the St Helens Council Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- That users may only access Willow Bank's networks through a properly enforced password protection policy

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up-to-date awareness of e-safety matters and of the current Willow Bank e-safety policy and practices
- They have read, understood, and signed the Willow Bank School Staff Acceptable Use Policy/Agreement (AUP)
- They report any suspected misuse or problem to Nicola Laughton for investigation/action/sanction

Designation Person for Child Protection / Child Protection Officer

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
- An appropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

E-Safety Committee

Members of the E-safety committee will assist with:

- The production, review and monitoring of Willow Bank e-safety policy

Students Pupils

- Are responsible for using Willow Bank Schools ICT systems and mobile technologies in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to systems
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

Parents Carers

Willow Bank will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/Learning Platform and information about national/local e-safety campaigns/literature. Parents and carers will be responsible for:

- Endorsing (by signature) the Student/Pupil Acceptable Use Policy

Community Users

Community Users who access ICT systems or Learning Platform as part of the Extended School provision will be expected to sign a Community User Acceptable Use Policy (AUP) before being provided with access to school systems.

6. E-Safety Education and Training

Education – students / pupils

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

- A planned e-safety programme will be provided as part of ICT/PHSE/other lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in and outside school.
- Key e-safety messages will be reinforced as part of a planned programme of assemblies, enrichment, and pastoral activities
- Students/pupils will 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

7. Why is Internet Use Important?

The rapid developments in electronic communications are having many effects on society. Through ICT and Internet use Willow Bank School are aiming to equip our pupils with the tools needed to develop both skills for life such as effective information gathering with a view to sources and reliability but also prepare pupils for possible jobs where ICT basics such as word processing, Spreadsheets, desk top publishing etc. may be required.

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business, and social interaction. Willow Bank has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside Willow Bank and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in Willow Bank is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance Willow Bank's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use

8. How Does Internet Use Benefit Education?

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries.
- Inclusion in the National Education Network which connects all UK schools.
- Educational and cultural exchanges between pupils worldwide.
- Vocational, social and leisure use in libraries, clubs and at home.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments, educational materials, and effective curriculum practice.
- Collaboration across networks of schools, support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.

9. How Can Internet Use Enhance Learning?

Increased computer numbers and improved Internet access may be provided but its impact on pupils learning outcomes should also be considered. Developing effective practice in using the Internet for teaching and learning is essential. Pupils need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught. Methods to detect plagiarism may need to be developed.

- Willow Bank Schools Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval, and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

10. How Will Pupils Learn to Evaluate Internet Content?

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read.

Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy etc. provide an opportunity for pupils to develop skills in evaluating Internet content. For example, researching the Holocaust will undoubtedly lead to Holocaust denial sites which teachers must be aware of.

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

11. Education and 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 formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand Willow Bank e-safety policy and Acceptable Use Policies

12. How Will Information Security Systems Be Maintained?

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

Local Area Network (LAN) Security Issues include

- Users must act reasonably — e.g., the downloading of large files during
- The working day will affect the service that others receive.
- Users must take responsibility for their network use. For Willow Bank staff, flouting electronic use policy is regarded as a reason for discipline procedures.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

Wide Area Network (WAN) Security Issues include

- St Helens Broadband firewalls and local CPEs are configured to prevent unauthorised access between schools/academies.
- Decisions on WAN security are made on a partnership between Agilisys and St Helens

Willow Bank School's Broadband network is protected by a cluster of high-performance firewalls at the Internet connecting nodes in St Helens Council. These industry leading appliances are monitored and maintained by a specialist security command centre.

The security of Willow Bank information systems and users will be reviewed regularly.

- Virus protection will be updated regularly.
- Portable media may not be used without specific permission followed by an anti-virus / malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on Willow Bank's network will be regularly checked.

- The ICT coordinator/network manager (Agilisys) will review system capacity regularly.
- The use of user logins and passwords to access Willow Bank network will be enforced.

13. How Will Email Be Managed?

Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits; interesting projects between schools/academies in neighboring villages and in different continents can be created, for example.

The implications of email use for Willow Bank and pupils need to be thought through and appropriate safety measures put in place. Unregulated email can provide routes to pupils that bypass the traditional boundaries.

In Willow Bank School context (as in the business world), email should not be considered private, and most schools/academies and many firms reserve the right to monitor email.

There is a balance to be achieved between necessary monitoring to maintain the safety of pupils and staff and the preservation of human rights, both of which are covered by recent legislation.

It is important that staff understand they should be using a work provided email account to communicate with parents/carers, pupils, and other professionals for any official school business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

The use of email identities such as john.smith@sthelens.org.uk generally needs to be avoided for younger pupils, as revealing this information could potentially expose a child to identification by unsuitable people.

Email accounts should not be provided which can be used to identify both a student's full name and their school. Secondary schools should limit pupils to email accounts approved and managed by Willow Bank. For primary schools, whole-class or project email addresses should be used.

When using external providers to provide students with email systems, schools must pay close attention to the sites terms and conditions as some providers have restrictions of use and age limits for their services. Spam, phishing, and virus attachments can make email dangerous.

Willow Bank School can monitor use via logins.

- Pupils may only use approved email accounts for Willow Bank purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission from an adult.
- Staff will only use official Willow Bank School provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Access to Willow Bank external personal email accounts *may* be blocked.
- Email sent to external organisations should be written carefully and authorised before sending in the same way as a letter written on Willow Bank School headed paper would be.

14. How Will Published Content be Managed?

Many schools have created excellent websites and communication channels, which inspire pupils to publish work of a high standard. Websites can celebrate pupils' work, promote Willow Bank, and publish resources for projects. Editorial guidance will help reflect Willow Bank's requirements for accuracy and good presentation.

Sensitive information about schools and pupils could be found in a newsletter but a school website is more widely available. Publication of any information online should always be considered from a personal and school security viewpoint.

- Material such as staff lists, or a school plan may be better published in Willow Bank handbook or on a secure part of the website which requires authentication.
- The contact details on the website should be Willow Bank address, email, and telephone number. Staff or pupils' personal information must not be published. Email addresses will be published carefully online, to avoid being harvested for spam (e.g., by replacing '@' with 'AT'.)
- The head teacher will take overall editorial responsibility for online content published by Willow Bank School and will ensure that content published is accurate and appropriate.
- Willow Bank School website will comply with guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

15. Can Pupils' Images and Work be Published?

Still and moving images and sound add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless, the security of staff and pupils is paramount. Although common in newspapers, the publishing of pupils' names with their images is not acceptable. Published images could be reused, particularly if large images of individual pupils are shown.

Strategies include using relatively small images of groups of pupils and possibly even using images that do not show faces at all. "Over the shoulder" can replace "passport style" photographs but still convey the educational activity. Personal photographs can be replaced with self-portraits or images of pupils' work or of a team activity. Pupils in photographs should, of course, be appropriately clothed.

Images of a pupil should not be published without the parent's or carer's written permission. Some schools ask permission to publish images of work or appropriate personal photographs on entry, some once a year, others at the time of use. Pupils also need to be taught the reasons for caution in publishing personal information and images online.

Please see the Children's Safeguards site, "Use of photographic images of children" sthelenslscb.org.uk/

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Pupils' work can only be published with their permission or the parents.
- Written consent will be kept by Willow Bank where pupils' images are used for publicity purposes until the image is no longer in use.

16. How Will Social Networking, Social Media and Personal Publishing be Managed?

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

For responsible adults, social networking sites provide easy to use, free facilities, although advertising often intrudes, and some sites may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers, and the difficulty of removing an inappropriate image or information once published.

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Examples of social media and personal publishing tools include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger, and many others.

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

17. How Will Filtering be Managed?

Levels of Internet access and supervision will vary according to the pupil's age and experience. Access profiles must be appropriate for all members of Willow Bank community. Older secondary pupils, as part of a supervised project, might need to access specific adult materials; for instance, a course text or set novel might include references to sexuality.

Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised, and restrictions removed temporarily. Systems to adapt the access profile to the pupil's age and maturity are available.

Access controls fall into several overlapping types (commonly described as filtering):

- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day. This typically will be done by St Helens Council.
- A walled garden or "allow list" restricts access to a list of approved sites. Such lists inevitably limit pupils' access to a narrow range of content.
- Dynamic content filtering examines web page content or email for unsuitable words.
- Keyword lists filter search engine searches and URLs for inappropriate results and web addresses.
- Rating systems give each web page a rating for sexual, profane, violent, or other unacceptable content. Web browsers can be set to reject rated pages exceeding a threshold.
- URL monitoring records the Internet sites visited by individual users. Reports can be produced to investigate pupil access.
- Key loggers record all text sent by a workstation and analyse it for patterns.

Schools installing or managing their own filtering systems and policies must be aware of the responsibility and demand on management time. Thousands of inappropriate sites are created each day and many change URLs to confuse filtering systems. It is the Senior Leadership Team's responsibility to ensure appropriate procedures are in place and all members of staff are suitably trained to supervise Internet access. It is important that school recognise that filtering is not 100% effective. There are ways to bypass filters (such as using proxy websites, using a device not connected to the network e.g., mobile phone).

Occasionally mistakes may happen, and inappropriate content may be accessed. It is therefore important that children should always be supervised when using internet access and that Acceptable Use Policies are in place. In addition, Internet Safety Rules should be displayed, and both children and adults should be educated about the risks online. There should also be an Incident Log to report breaches of filtering or inappropriate content being accessed. Procedures need to be established to report such incidents to parents and St Helens Council (The Schools Broadband Service Desk at EiS or the e-Safety Officer) where appropriate. Any material that Willow Bank believes is illegal must be reported to appropriate agencies.

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

- Willow Bank's broadband access will include filtering appropriate to the age and maturity of pupils.
- Willow Bank will work with St Helens / Agilisys and Willow Bank's Broadband team to ensure that filtering policy is continually reviewed.
- Willow Bank will have a clear procedure for reporting breaches of filtering. All members of Willow Bank community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to Willow Bank e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- Willow Bank filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to Willow Bank filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- Willow Bank Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that Willow Bank believes is illegal will be reported to appropriate agencies such as St Helens Council
- Willow Bank's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

18. Communication Devices and Methods

The following table shows Willow Bank's policy on the use of communication devices and methods.

Where it is indicated that the method or device is allowed at certain times, these are clearly outlined in the next table.

	Staff & other adults				Students/Pupils			
Communication method or device	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 Willow Bank								☒
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 personal handheld devices e.g., PDAs, PSPs				☒				☒
Use of personal email addresses Willow Bank, or on Willow Bank network		☑						☒
Use of Willow Bank email for personal emails				☒				☒
Use of chat rooms / facilities				☒				☒
Use of instant messaging				☒				☒
Use of social networking sites				☒				☒
Use of blogs		☑				☑		

This table indicates when some of the methods or devices above may be allowed:

	Circumstances when these may be allowed	
Communication method or device	**Staff & other adults**	**Students/Pupils**
Mobile phones may be brought to Willow Bank	Staff and other adults can bring mobile phones into Willow Bank	Pupils can bring mobile phones into Willow Bank as long as they are handed to reception during am registration for safety. These will be handed back to pupils at the end of the day.
Use of mobile phones in lessons	Switched off during teaching time	Phones already handed in
Use of mobile phones in social time	e.g., during breaks or after Willow Bank	Phones already handed in
Taking photos on personal mobile phones or other camera devices	Professional conduct	Phones already handed in
Use of personal handheld devices e.g., PDAs, PSPs	Yes, in class and in personal time	School devices only to be used and as directed by staff.
Use of personal email addresses in school, or on Willow Bank network	e.g., during breaks or after Willow Bank	Not allowed
Use of Willow Bank email for personal emails	Not allowed	During planned ICT activities
Use of chat rooms / facilities	Not allowed	Not allowed
Use of instant messaging	Not allowed	Not allowed
Use of social networking sites	Not allowed	Not allowed
Use of blogs	Not allowed	Only ones set up by subject tutors on the VLE so that they can be monitored.

19. Unsuitable Inappropriate Activities

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

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
User Actions	☑			☒	☒
Child sexual abuse images					☒
Promotion or conduct of illegal acts, e.g., 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 based on race, gender, sexual orientation, religion and belief, age, and disability					☒
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 Willow Bank or brings Willow Bank into disrepute				☒	
Using Willow Bank systems to run a private business				☒	
Use systems, applications, websites, or other mechanisms that bypass the filtering or other safeguards employed by LSCB and / or Willow Bank				☒	
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 (e.g., financial / personal information, databases, computer / network access codes and passwords)				☒	

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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				☒	
Use of social networking sites				☒	
Use of video broadcasting e.g., YouTube	☑				
Accessing the internet for personal or social use (e.g., online shopping/ social media including Twitter)				☒	
Using external data storage devices (e.g., USB) that have not been encrypted (password protected and checked for viruses				☒	

20. Good Practice Guidelines

Email

Best practice

☑ **DO**

Staff and students/pupils should only use their school email account to communication with each other.

Safe practice

Check Willow Bank e-safety policy regarding use of your school email or the internet for personal use e.g., shopping.

Poor practice

☒ **DO NOT**

Staff: don't use your personal email account to communicate with students/pupils and their families without a manager's knowledge or permission – and in accordance with the e-safety policy.

Images, Photos and Videos

Best practice

☑ DO

Only use school equipment for taking pictures and videos.

Ensure parental permission is in place.

Safe practice

Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to Willow Bank network immediately after the event.

Delete images from the camera/device after downloading.

Poor practice

☒ DO NOT

Don't download images from organisation equipment to your own equipment.

Don't use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the e-safety policy.

Don't retain, copy, or distribute images for your personal use.

Internet

Best practice

☑ **DO**

Understand how to search safely online and how to report inappropriate content.

Safe practice

Staff and students/pupils should be aware that monitoring software will log online activity.

Be aware that keystroke monitoring software does just that. This means that if you are online shopping then your passwords, credit card numbers and security codes will all be visible to the monitoring technicians

Poor practice

☒ **DO NOT**

Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings

Breach of the e-safety and acceptable use policies may result in confiscation of equipment, closing of accounts and instigation of sanctions.

Mobile Phones

Best practice

☑ DO

Staff: If you need to use a mobile phone while on school business (trips etc), Willow Bank will/ should provide equipment for you. Make sure you know about inbuilt software/ facilities and switch off if appropriate.

Safe practice

Check the e-safety policy for any instances where using personal phones may be allowed.

Staff: Make sure you know how to employ safety measures like concealing your number by dialling 141 first

Poor practice

☒ DO NOT

Staff: Don't use your own phone without the Headteacher/SLT knowledge or permission. Don't retain service student/pupil/parental contact details for your personal use.

Social Networking (E.G. Facebook/ Twitter)

Best practice

☑ DO

If you have a personal account, regularly check all settings, and make sure your security settings are not open access. Ask family and friends to not post tagged images of you on their open access profiles.

Safe practice

Don't accept people you don't know as friends. Be aware that belonging to a 'group' can allow access to your profile.

Poor practice

☒ DO NOT

Don't have an open access profile that includes inappropriate personal information and images, photos, or videos.

Staff:

- Don't accept students/pupils or their parents as friends on your personal profile.
- Don't accept ex-students/pupils' users as friends.
- Don't write inappropriate or indiscrete posts about colleagues, students/pupils, or their parents.

Webcams

Best practice

☑ DO

Make sure you know about inbuilt software/ facilities and switch off when not in use.

Safe practice

Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission. Make arrangements for pictures to be downloaded to Willow Bank network immediately after the event.

Delete images from the camera/device after downloading.

Poor practice

☒ DO NOT

Don't download images from organisation equipment to your own equipment. Don't use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the e-safety policy.

Don't retain, copy, or distribute images for your personal use.

21. Incident Management

Incidents (students/pupils):	Refer to class teacher	Refer to MLT / 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 e.g., 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 / another handheld device	✓	✓	✓						✓
Unauthorised use of social networking/ instant messaging/personal email	✓	✓	✓						✓
Unauthorised downloading or uploading of files	✓				✓			✓	✓
Allowing others to access Willow Bank network by sharing username and passwords		✓				✓		✓	✓
Attempting to access or accessing Willow Bank network, using another student's/pupil's account		✓				✓		✓	✓
Attempting to access or accessing Willow Bank 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 Willow Bank into disrepute			✓			✓			✓

Incidents (students/pupils):	Refer to class teacher	Refer to MLT / 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 e.g., detention / exclusion
or breach the integrity of the ethos of Willow Bank									
Using proxy sites or other means to subvert Willow Bank's filtering system					✓		✓		
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓						✓	
Deliberately accessing or trying to access offensive or pornography		✓	✓		✓		✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act								✓	

Incidents (staff and community users):	Refer to MLT / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Removal of network / internet access rights	Warning	Further sanction *(please state)*
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	✓		✓			✓	
Unauthorised downloading or uploading of files				✓			
Allowing others to access Willow Bank network by sharing username and passwords or attempting to access or		✓		✓		✓	

Incidents (staff and community users):	Refer to MLT / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Removal of network / internet access rights	Warning	Further sanction *(please state)*
accessing Willow Bank network, using another person's account							
Careless use of personal data e.g., 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		✓				✓	
Actions which could compromise the staff member's professional standing	✓		✓		✓	✓	
Actions which could bring Willow Bank into disrepute or breach the integrity of the ethos of Willow Bank		✓			✓	✓	
Using proxy sites or other means to subvert Willow Bank'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		✓	✓		✓		

22. Further Information and Support

For a glossary of terms used in this document:
http://www.sthelens.gov.uk/what-we-do/schools-and-education/e-safety/secondary-schools/

For e-Safety Practice Guidance for those who Work and Volunteer with, and have a Duty of Care to Safeguard Children and Young People:
http://sthelens.gov.uk/esafety

R u cyber safe?
E-safety tips about how to stay safe online:
http://rucybersafe.info

Appendix 1 Student Pupil AUP

Student/Pupil Acceptable Use Policy Agreement

This Acceptable Use Policy is intended to make sure:

- That you will be a responsible user and stay safe while using the internet and other technology for learning and personal use
- That ICT systems and users are protected from accidental or deliberate misuse

Willow Bank will try to ensure that you will have good access to ICT to enhance your learning and will, in return, expect you to agree to be a responsible user.

Please make sure you read and understand the following ☑ **I WILL** and ☒ **I WILL NOT** statements. If there's anything you're not sure of, ask your teacher.
This form relates to the student/pupil Acceptable Use Policy (AUP), to which it is attached.

☑ I WILL:

- Treat my username and password like my toothbrush – I will not share it, or try to use any other person's username and password
- Immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online
- Respect others' work and property and will not access, copy, remove or change anyone else's files, without their knowledge and permission
- 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
- Only use my personal handheld/external devices (mobile phones/USB devices etc) in school if express permission has been granted as part of an emergency or as part of a structured lesson.
- Immediately report any damage or faults involving equipment or software, however this may have happened

☒ I WILL NOT:

- Try (unless I have permission) to make downloads or uploads from the Internet
- Take or share images (pictures and videos) of anyone without their permission
- Use Willow Bank ICT systems for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g., YouTube), unless I have permission of a member of staff to do so.
- Try to upload, download, or access any materials which are illegal or inappropriate or may cause harm or distress to others
- 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
- 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
- Attempt to install programmes of any type on a machine, or store programmes on a computer
- Try to alter computer settings
- Download music / images / videos etc from an external hard drive onto Willow Bank network.

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

- I understand that Willow Bank 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 Willow Bank and where they involve my membership of Willow Bank community (examples would be cyber-bullying, use of images or personal information)
- I understand that if I fail to follow this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to Willow Bank network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police
- I have read and understand the above and agree to follow these guidelines when:
- I use Willow Bank ICT systems and equipment (both in and out of Willow Bank)
- I can't use my own equipment in Willow Bank e.g., mobile phones, PDAs, cameras etc
- I use my own equipment out of Willow Bank in a way that is related to me being a member of Willow Bank e.g., communicating with other members of Willow Bank, accessing Willow Bank email, Learning Platform, website etc

(Parents/carers are requested to sign the permission form below to show your support of Willow Bank in this important aspect of Willow Bank's work).

Name of Student/Pupil		
Group/Class		
Signed (Student/Pupil)		Date
Signed (Parent/Carer)		Date

Appendix 2 Staff, Volunteer, Community User AUP

School Policy

This Acceptable Use Policy (AUP) is intended to ensure:

- That staff, volunteers and community users will be responsible users and stay safe while using the internet and other communications technologies for educational, personal, and recreational use.
- That Willow Bank ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff, volunteers and community users are protected from potential risk in their use of ICT in their everyday work.

Willow Bank will try to ensure that staff, volunteers, and community users will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff, volunteers and community users to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use Willow Bank 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 recognise the value of the use of ICT for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of ICT.

I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that Willow Bank will monitor my use of the ICT systems, email, and other digital communications.
- I understand that the rules set out in this agreement also apply to use of Willow Bank ICT systems (e.g., laptops, email, etc) out of Willow Bank.
- I understand that Willow Bank ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by Willow Bank.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate, or harmful material or incident I become aware of, to the appropriate person.
- I will be professional in my communications and actions when using Willow Bank ICT systems:
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with Willow Bank's policy on the use of digital/video images. I will not use my personal equipment to record these images unless I have permission to do so. Where these images are published (e.g., on Willow Bank website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use chat and social networking sites in Willow Bank in accordance with Willow Bank's policies.
- I will only communicate with students/pupils and parents/carers using official Willow Bank systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- Willow Bank and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of Willow Bank:
- When I use my personal handheld/external devices (PDAs/laptops/mobile phones/USB devices etc) in Willow Bank, I will follow the rules set out in this agreement, in the same way as if I was using Willow Bank equipment. I will also follow any additional rules in line with Willow Bank's E-Safety Policy set by Willow Bank about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant Willow Bank policies.
- I will not try to upload, download, or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not 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 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 install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in Willow Bank policies.
- I will not disable or cause any damage to Willow Bank equipment, or the equipment belonging to others. will only transport, hold, disclose, or share personal information about myself or others, as outlined in the Willow Bank/Local Authority Personal Data Policy. Where personal data is transferred outside the secure Willow Bank network, it must be encrypted.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Willow Bank policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.

When using the internet in my professional capacity or for Willow Bank sanctioned personal use:

- I will 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 download or distribute copies (including music and videos)

Staff, Volunteer and Community User Acceptable Use Agreement Form

This form relates to the student/pupil Acceptable Use Policy (AUP), to which it is attached.
I understand that I am responsible for my actions in and out of Willow Bank:

- I understand that this Acceptable Use Policy applies not only to my work and use of Willow Bank ICT equipment in Willow Bank, but also applies to my use of Willow

Bank ICT systems and equipment out of Willow Bank and my use of personal equipment in Willow Bank or in situations related to my employment by Willow Bank.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police

I have read and understood Willow Bank's E-safety Policy

I have read and understand the above and agree to use Willow Bank ICT systems (both in and out of Willow Bank) and my own devices (in Willow Bank and when carrying out communications related to Willow Bank) within these guidelines.

Name	
Position	
Signed	
Date	

Appendix 3 Use of Images Consent Form

Use of Digital / Video Images

The use of digital/video images plays an important part in learning activities. Students/Pupils and members of staff may be using digital or video cameras to record evidence of activities in lessons and out of Willow Bank. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on Willow Bank website and occasionally in the public media.

Willow Bank will comply with the Data Protection Act and request parents / carers permission before taking images of members of Willow Bank. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

Parents are requested to sign the permission form below to allow Willow Bank to take and use images of their children.

Permission Form

Parent / Carers Name	
Student / Pupil Name	

As the parent / carer of the above student / pupil, I agree to Willow Bank taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of Willow Bank.

I agree that if I take digital or video images at, or of, Willow Bank events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed	
Date	

Appendix 4 Connecting Policies for Safeguarding Purposes

Willow Bank School believes it is very important that policies relating to Safeguarding issues, across the school, are read in conjunction between one another. The Policies in question have been listed below.

- Safeguarding Policy
- Child Protection Policy
- Safer Recruitment Policy
- Health & safety Policy
- Drug Policy
- First Aid Policy
- Anti-bullying & harassment Policy
- Behaviour Policy
- Positive Handling and Guidance Policy
- Attendance Policy
- E-safety Policy
- Lone Worker Policy