E-Safety Policy

(Parent)

Approved By	Strategy and Resources Committee
Date Approved	15th November 2023
Last Revised	October 2023
Review Date	October 2025

Writing and reviewing the e-safety policy

The E-Safety Policy relates to other policies including, Child Protection and Anti-Bullying.

- The school's e-safety co-ordinator, is also the Child Protection Designated Lead, as the roles overlap.
- Our E-Safety Policy has been written by the school, building on best practice and government guidance.
- It has been agreed by senior management and approved by the Local Academy Board (LAB). The E-Safety Policy and its implementation will be reviewed annually.

Teaching and Learning

Why internet and digital communications are important

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and students.
- The school internet access is provided by Shropshire Council through a regional broadband contract, which includes filtering appropriate to the age of students.
- Students will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Students will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Students will be shown how to publish and present information appropriately to a wider audience.

Students will be taught how to evaluate internet content

- The school will seek to ensure that the use of internet derived materials by staff and by students complies with copyright law.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Students will be taught how to report inappropriate internet content e.g. using the CEOP Report Abuse icon.
- For students whose parents/carers lack economic or cultural educational resources, the school should build digital skills and resilience, acknowledging the lack of experience and internet at home.
- For children with social, familial or psychological vulnerabilities, further consideration should be taken to reduce potential harm.

Managing internet Access

Information system security

- School ICT systems security will be reviewed regularly.
- At Ludlow CE School, we use the web filtering software *Smoothwall* to block harmful and inappropriate content. See Appendix 4.
- Virus protection will be updated regularly, through Microsoft Defender.
- Security strategies will be discussed with Shropshire ICT and The Diocese of Hereford Multi-Academy Trust (DHMAT).
- Passwords should be changed regularly and must not be shared.
- In line with or Data Protection protocols, staff must always 'lock' a device if they are going to leave it unattended.
- Only encrypted USB pens are to be used in school. Students must seek permission before using a USB pen.

E-mail

- Students and staff may only use approved e-mail accounts on the school system, with personal log-ins.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details or images of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff to student email communication must only take place via a school email address or from within the learning platform, and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from students to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the website should be the school address, email and telephone number. Staff email will be made available, also. Staff or students' personal information will not be published.
- The Headteacher, or nominee, will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing students' images and work

- Photographs that include students will be selected carefully. The school will use photographs only when permission has been granted by the parent/carer.
- Students' full names will be avoided on the website or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
- Written permission from parents or carers will be obtained as part of the admission process, before photographs of students are published on the school website.

Social networking and personal publishing on the school learning platform

- The school has a robust social media policy.
- The school will access social media sites if concerns are raised, and educate students in their safe use e.g. use of passwords.
- Students will be advised never to give out personal details of any kind which may identify them or their location, or place personal photos on any social network space provided in the school learning platform.
- Students and parents will be advised that the use of social network spaces outside school brings a range of opportunities; however, it does present dangers for primary and secondary aged students.

Filtering and Monitoring systems

- The school must ensure that its filtering and monitoring systems are fit for purpose; this is part of the role of the Designated Safeguarding Lead.
- All staff must understand their role and responsibilities around filtering and monitoring as part of safeguarding training.
- The school will work in partnership with Shropshire ICT and DHMAT to ensure systems to protect students are reviewed and improved.
- The school use the web filtering software, *Smoothwall*, to block harmful and inappropriate content.
- An email alert is sent to the DSL and DDSL of any potential misuse by students.
- A log of any incidents will help staff to identify patterns and behaviours of the students.
- See Appendix 4 for the Filtering and Monitoring Protocol and flowchart of actions.
- If staff or students come across unsuitable on-line materials, the site must be reported to the E-Safety Coordinator and/or the ICT Technician.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing and Remote Learning (if required) – using Microsoft Teams

- Videoconferencing will use the educational broadband network to ensure quality of service and security.
- MS Teams must be used when delivering learning remotely to students.
- All videoconferencing will be managed and supervised by the teacher.
- The students should join the session on their own, without family members present.
- Students will need to turn off their camera and microphone, unless directed to use these facilities by the class teacher.
- Screenshots of any live meetings must not be taken or shared on social media, under any circumstances.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity, and with the permission of the teacher.
- The sending of abusive or inappropriate text messages is forbidden.
- Handheld technologies, including games and mobile phones, often have internet access which may not include filtering. Care will be taken with their use within the school.
- Staff will use a school phone where contact with students is required.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the General Data Protection Regulations 2018.

Policy Decisions

Authorising internet access

- All staff, LAB members and visitors must read and sign the "Acceptable Internet and Computer Use Policy for Staff, LAB Members and Visitors" before using any school ICT resource. (Appendix 1)
- The school will maintain a current record of all staff and students who are granted access to school ICT systems.
- Parents/carers will be asked to sign to acknowledge they have read and agreed to the "Acceptable Internet and Computer Use Policy for Students" (Appendix 2) when their child joins the school.
- Students must agree to comply to the "Acceptable Use of the Internet Statement" when applying for internet access. (Appendix 3)

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor DHMAT can accept liability for the material accessed, or any consequences of internet access.
- The school will monitor ICT use to establish if the e-safety policy is adequate and that the implementation of the E-Safety Policy is appropriate and effective.

Handling e-safety complaints

- Complaints of internet misuse will be overseen by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a Child Protection nature must be dealt with in accordance with the school's safeguarding procedures.
- Students and parents will be informed of the complaints procedure.
- Students and parents will be informed of consequences and sanctions for students misusing the internet, and this will be in line with the school's Behaviour Policy.

Introducing the E-Safety Policy to students

- Appropriate elements of the E-Safety policy will be shared with students as part of the induction process in Year 7, and further curriculum opportunities will be provided for students to gain awareness of e-safety issues and how best to deal with them. This will be addressed each year as students become more mature and the nature of newer risks can be identified.
- E-safety rules will be posted in all networked rooms.
- Students will be informed that network and internet use, will be monitored.

Staff and the E-Safety Policy

- All staff will be advised of the school's E-Safety Policy and its importance explained.
- All staff will sign to acknowledge that they have read and understood the E-Safety Policy and agree to work within the agreed guidelines.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff will be advised on the use of social media, both at work and in their personal situation.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management, including the Designated Safeguarding Lead, and have clear procedures for reporting issues.

Enlisting parents' support

- Parents' and carers' attention will be drawn to the school's E-Safety Policy in newsletters and on the school website and updates will be given.
- The school will ask all new parents/carers to sign the parent /student agreement when their child begins school.
- Parents are offered e-safety training, as required, with a focus on education and having an overview of tools to allow them to take control whilst not undermining trust.

Appendices:

1. Staff, LAB Members and Visitors Acceptable Use of Internet and Computer Statement
2. Acceptable Internet and Computer Use Statement for All Students
3. Acceptable Use of the Internet – Student's Agreement
4. Filtering and Monitoring Protocol

Staff, LAB Members and Visitor Acceptable Use of Internet and Computer Statement

Ludlow CE School

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This statement is designed to ensure that all staff are aware of their professional responsibilities, and those under the General Data Protection Act, when using any form of ICT. All staff are expected to sign this statement and adhere at all times to its contents. Any concern or clarification should be discussed with Mrs Deb Tysall, E-safety Co-ordinator or Rowena Morris, Data Protection Officer.

- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.

- I will comply with the ICT system security and not disclose or share any passwords provided to me by the school or other related authorities.

- I will only use the school's email, internet and any related technologies for professional purposes, or for uses deems 'reasonable' by the Headteacher or Local Academy Board.

- I will not install any hardware or software without the permission of the Headteacher or School Business Manager.

- I will not browse, download, upload or distribute any materials that could be considered offensive, illegal or discriminatory.

- I understand that all my use of the internet, and other related technologies, will be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.

- I will respect copyright and intellectual property rights.

- Images of students and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network/learning platform without the permission of the parent/carer, member of staff or Headteacher.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

- I will ensure that all electronic communications with parents, students and staff, including email, IM and social networking, are compatible with my professional role, and that a message cannot be misunderstood or misinterpreted. Staff should not make contact with students or parents through personal email, by text or personal phones, or on social media sites. Any communication outside of the school network, containing identifiable data, will be sent in an encrypted format.

- I will support the school's E-Safety Policy and help students to be safe and responsible in their use of ICT and related technologies. I will promote e-safety with students in my care and will help them to develop a responsible attitude to system- use, communication and publishing.

- I will report any incidents of concern regarding children's safety to the School Business Manager, the Child Protection Designated Lead or Headteacher.

- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures, and serious infringements may be referred to the Police.

User Signature

I agree to follow this Acceptable Use Statement and to support the safe use of ICT throughout the school.

Full Name …….. (Printed)

Job Title ……..

Signature …… Date ……..

ACCEPTABLE INTERNET & COMPUTER USE STATEMENT FOR ALL STUDENTS

The computer system is owned by the school and/or DHMAT and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties - the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Neither the school nor DHMAT will be liable under any circumstances for any injury, distress, loss or damage to the student or the parents, which may arise directly or indirectly from the student's use of the Internet facilities, the use of e-mail, or from other students' unauthorised use of those facilities or e-mail.

- Permission will be sought from students and parents before any personal data, i.e. names and photographs, are published on a web site;
- Access must only be made via the authorised account and password, which must not be made available to any other person;
- All Internet use should be appropriate to staff professional activity or student's education;
- The downloading of sexist, racist, pornographic, indecent or abusive images, text or sound files is forbidden;
- The downloading of any program, screen saver, game etc. without permission from an authorised person is forbidden;
- Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems, is forbidden;
- Sites and materials accessed must be appropriate to work in school; users will recognise materials that are inappropriate and should expect to have their access removed;
- Users are responsible for e-mail they send and for contacts made that may result in e-mail being received;
- The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded;
- The sending of 'sensitive personal data' whether relating to the sender or not is forbidden unless it is processed for reasons outlined in the school Data Protection Policy and the GDPR regulations 2018.
- The sending of any information which students are not certain to be 'public knowledge' outside the school is forbidden;
- Posting anonymous messages and forwarding chain letters is forbidden;
- Copyright of materials and intellectual property rights must be respected;
- Legitimate private interests may be followed, providing school use is not compromised;
- No unauthorised contract, purchase or payment should be made over the Internet;
- Student purchases over the Internet are forbidden;
- Students are forbidden to access social networking sites, such as Instagram, TikTok, Snapchat or Facebook;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Staff and students should be aware that Internet access is filtered and monitored and concerns are reported to the Headteacher.

ACCEPTABLE USE OF THE INTERNET

Student's Agreement

You must have the written permission of a parent or carer before you can use the internet in school.

You are only able to use it to access materials for use in lessons and to help with your learning. The school will keep a record of the times you use the internet and all the sites you have visited.

The school use the web filtering software, *Smoothwall*, to block harmful and inappropriate content. An email alert is sent to a senior member of staff if there is misuse of the internet by a student.

I agree to the following:

- I will only use the internet for school work and will not visit social networking sites, chat rooms or any other unsuitable sites
- I will not access any areas of the internet that are inappropriate or offensive
- If any unsuitable material appears when I am using the internet I will report it to a teacher
- I accept responsibility to keep copyrighted material from being downloaded into the school
- I will not give personal information including credit card numbers, postal or email addresses, telephone or fax numbers, or use photographs of any other students, any adult or myself.
- I will always respect the privacy of files of other users. I will not enter the file areas of any other person
- I will not disclose any password or login name to anyone, other than the person responsible for running and maintaining the system
- I will be polite and use appropriate language in all my ICT communications
- I agree to staff having the right to view any material I use in the school's computers
- If I use material in my work, I will always list this in a bibliography. I will select the information I need and present it in my own words
- I will not damage computers, computer systems or networks
- If I break any of the terms of this agreement, I know that one or more of the following will result:
- A ban, temporary or permanent on the use of the internet facilities at school
- A letter informing my parents or carers of the rules I have broken
- Appropriate sanctions and restrictions placed on access to other school facilities
- Any other action decided by the Headteacher and Local Academy Board of the school.

User Signature

I agree to follow this Acceptable Use Statement and to support the safe use of ICT throughout the school.

Full Name …….. (Printed)

Signature …… Date ……..

Filtering and Monitoring Protocol

- At Ludlow CE School, we use the web filtering software, *Smoothwall*, to block harmful and inappropriate content and send an email alert to the DSL and DDSL of any potential misuse by students.

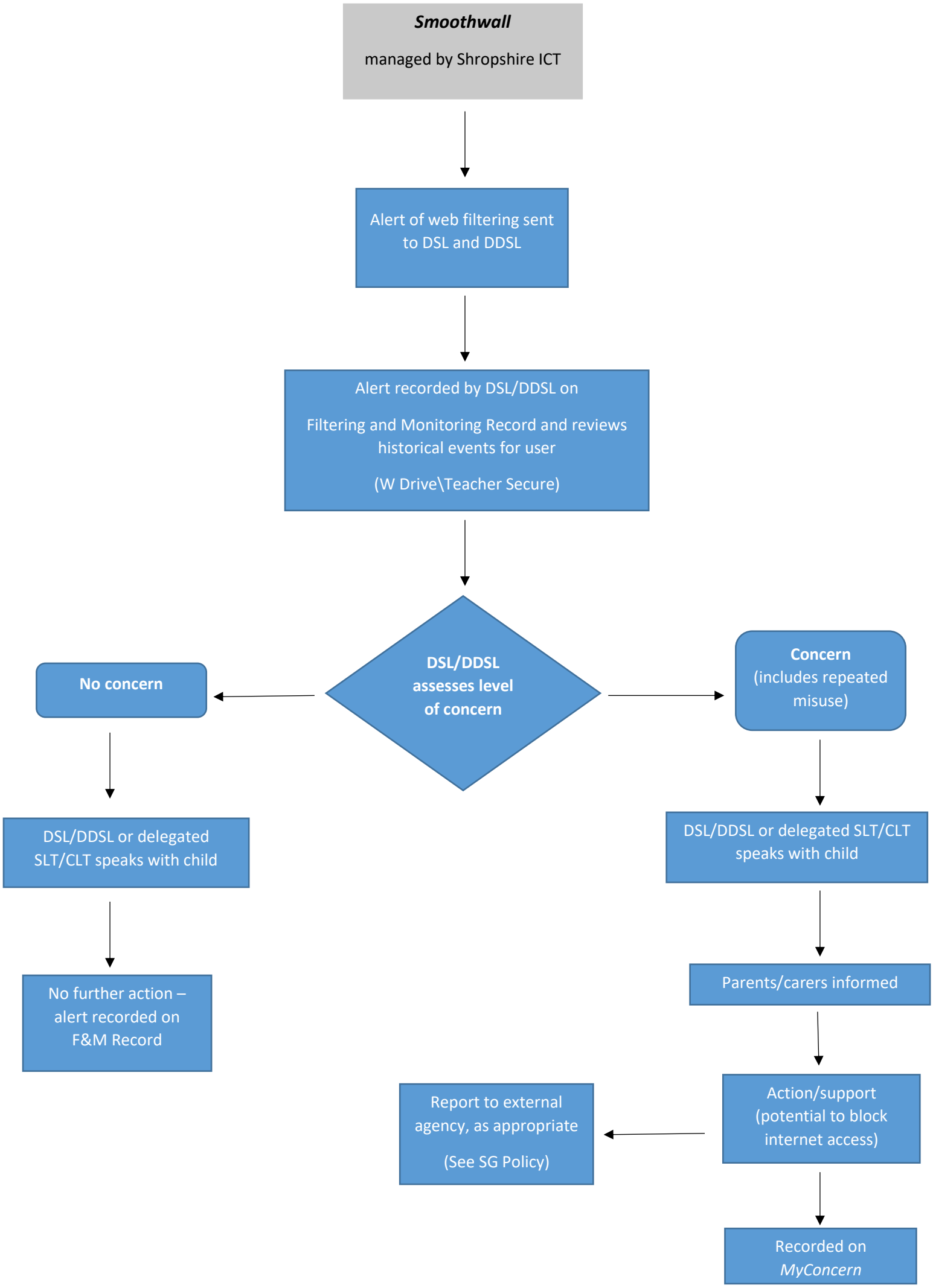
- All students use personal log-ins (not generic log-ins) so that the individual user who has attempted to access inappropriate material can be specifically identified.

- All alerts are logged, and actions recorded. Where necessary, an entry is made on *MyConcern* to ensure robust action and follow up is overseen by the DSL. (see flowchart)

- The web filtering software is linked to our main school internet feed, and protects all school owned devices, including laptops, PCs, iPads and Chromebook, whilst connected to the main school network. Safe search is enabled for our school on supported browsers (Chrome and Edge).

- The school reviews filtering and monitoring arrangements on a *termly* basis, to ensure technologies in place meet the school's safeguarding requirements (testfiltering.com)

- The school are able to get a view to what content is being blocked or allowed, and if rules need to be amended to better suit the individual user, year group or age. Any changes must be made by the DSL, with approval from the Headteacher, through Shropshire ICT's helpdesk (ict.support@shropshire.gov.uk)


Smoothwall
managed by Shropshire ICT
Alert of web filtering sent to DSL and DDSL
Alert recorded by DSL/DDSL on
Filtering and Monitoring Record and reviews historical events for user
(W Drive\Teacher Secure)
DSL/DDSL assesses level of concern
No concern
Concern (includes repeated misuse)
DSL/DDSL or delegated SLT/CLT speaks with child
No further action – alert recorded on F&M Record
DSL/DDSL or delegated SLT/CLT speaks with child
Parents/carers informed
Action/support (potential to block internet access)
Report to external agency, as appropriate
(See SG Policy)
Recorded on MyConcern

E-Safety Policy – Updates

Governors referred to as Local Academy Board (LAB) members	June 2021
Details around delivering removing learning	June 2021
Details around filtering and monitoring systems	October 2023