



Range High School

E-SAFETY

POLICY

Person responsible this policy: Assistant Headteacher (Safeguarding) / CAL - IT

Date of last review: May 2024

Date of next review: Summer Term 2025 – (major changes will be brought to the attention of trustees as, and when they occur)

RESPONSIBILITY FOR THIS POLICY HAS BEEN DELEGATED TO THE HEADTEACHER FOR ANNUAL REVIEW

General Information

Trustees: This section will be reviewed annually by the full governing board

Headteacher: Mr M McGarry

SLT: Mrs J McGugan – Assistant Headteacher - Safeguarding

SMT: CAL Computing + E-Safety Lead (SAH)

Contents

Policy Statement

Definitions of Misuse

Safe Use of Technology

Roles and Responsibilities

E-safety in the Curriculum

Support from Parents/Carers

Responsibilities of Pupils

Complaints

Reviewing our Policy

Appendix A: Acceptable Use Policy (Pupils)

Appendix B: Acceptable Use Policy (Staff)

Appendix C: Home Access to SIMS Protocol

Section One:

Principles

1. The e-safety section covers the safe use of Information Communication Technology (ICT) both inside school such as using the computer network (including the school Wi-Fi) and outside school such as accessing the VLE, ClassCharts, SIMS, Google Classroom, school emails or the school website from home. This e-safety policy also covers both wired desktop PCs and wireless devices such as Chromebooks.
2. We at Range High School believe that ICT is an essential resource to support teaching and learning, as well as playing an important role in the everyday lives of young people and adults. We also believe that it is important to build in the use of these technologies in order to provide our pupils with the skills to access life-long learning and employment
3. We also recognise that such technology can also be misused (see Section Two)
4. We acknowledge Range High School has a responsibility to educate our pupils and staff about e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom (see Section Three)
5. We will educate our pupils, staff and families about possible misuse and will provide education, infrastructure and processes which support safe use of a variety of technologies
6. We will designate specific roles and responsibilities (see Section Four)
7. We will provide a discrete Computer Science curriculum which addresses these issues (see Section Five)
8. We will engage the support of families in this work (see Section Six)
9. We will have a defined complaints procedure for e-safety (see Section Eight)
10. We will require all users to agree to the AUP (see Appendix A and B)
11. We will require all staff to agree to the Home Access to SIMS Protocol (see Appendix C)
12. We will review our policy annually (see Section Nine)

Section Two:

Definitions of Misuse

Misuse refers to the use of technology that is excessive or problematic and to the detriment of the user, the recipient, those around them and/or third parties that are not directly involved but who may be affected by it.

For example:

- Sending unwelcome messages that are threatening or cause discomfort to others
- Taking pictures or filming of others which are then used to bully others or to make others feel threatened or embarrassed with pictures/video sent to other people.
- Making phone calls that include silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified
- Using email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them
- Chat room bullying involves sending menacing or upsetting responses to others when they are in a web-based chat room
- Bullying through instant messaging (IM) is an Internet-based form of bullying where children and young people are sent unpleasant messages as they conduct real-time conversations online, (i.e. Snapchat, Facebook Messenger, Whatsapp)
- Bullying via websites includes the use of defamatory blogs (web logs), personal websites and online personal polling sites.

Section Three:

Safe Use of Technology & Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- responsibility for technical security resides with SLT who may delegate activities to identified roles.
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the SLT/Network Manager/E-Safety Lead
- password policy and procedures are implemented. (consistent with guidance from the National Cyber Security Centre)
- the security of their username and password and must not allow other users to access the systems using their log on details.
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- all school networks and systems will be protected by secure passwords. Passwords must not be shared with anyone.
- there is a risk-based approach to the allocation of learner usernames and passwords.
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted

- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud.
- our school network manager is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the IT service team through face to face or email, as agreed.
- use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
- there are restrictions in place for removable media
- systems are in place to control and protect personal data and data is encrypted at rest and in transit. (See data protection policy for further information)
- guest users are provided with appropriate access to school systems based on an identified risk profile.

We will educate our pupils, staff and families to use the following technologies appropriately in the following manner:

Email:

- The school gives all students and staff their own e-mail account to use for all school business as a work based tool. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail
- Staff must inform a senior member of staff if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of their Computer Science curriculum in 7.1 and 8.1 Schemes of Work.
- However staff choose to access their school e-mail, whether using a computer in school, a school device outside of school or on non-school hardware devices, the same school e-safety policy apply.
- Staff and pupils should be aware that a log of all emails that are sent, received and forwarded are kept forever by gMail, even if they are deleted.

Internet Access:

- The school has students who will have supervised access to Internet resources (where reasonable) through the school's fixed internet technology and firewall security
- Staff will preview any recommended sites before use by students
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work

- The school's policy on the use of mobile phones in school is that they should not be seen or heard. However, students may be allowed, under controlled conditions supervised by staff to access their phone for short periods of time to complete a task, such as checking their ClassCharts app.
- Staff and pupils should be aware that all files that are stored on the VLE or on their Google Drive account are kept forever by Google, even if they are deleted.

Social Networking:

Social networking sites, if used responsibly can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture commercialism and the safeguarding issues that such sites pose.

- At present, the school endeavours to deny access to social networking sites to pupils within. Some staff members may have access to social networking sites to promote activities carried out in school.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites, to consider the appropriateness of any images they post due to the difficulty of removing an image once online and where they can go to get help to take it down.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals. Pupils are also advised to check their profile privacy settings on a regular basis to ensure their settings are still set to maximum following updates from the provider.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the school.

Monitoring and Filtering

The school uses a firewall called Smoothwall. This will monitor all incoming and outgoing transmission. Smoothwall has a database of millions of known websites and places each website into a category. The school blocks access to websites by category, such as websites that contain pornography, gambling or criminal activity.

All websites that are shown to staff or pupils have to be approved by the firewall. If the website is in a blocked category it is not shown and a log of this is kept. Serious offences are forwarded to the head of Computer Science / Julie McGugan / Heads of House / Head Teacher.

If a website is not blocked then additional checks are carried out by the firewall. Each website:

- Is given a category which is compared against the Smoothwall database. If they are different it is then blocked based on the Smoothwall block settings
 - Is given a rating and anything over 2 out of 5 is blocked
 - Is checked against our own internal blocked list
- If a website passes all of these then the website is shown.

The school also uses IMPERO/SENSO software to monitor activities carried out on the network. This software will take photographs of the screen if it thinks that a user has breached the conditions outlined in this policy. These will be forwarded to the e-safety coordinator and relevant heads of year.

The school acknowledges that whilst filtering and monitoring is an important part of schools online safety responsibilities, it is only one part of our role. Children and adults are likely to have access to systems external to the school control, such as mobile phones and other internet enabled devices and technology 3, 4 & 5G data.

As part of student's e-Safety curriculum, they are taught about networks. Students are taught about different apps that make use of their location, the dangers of sharing their location from their devices and how to turn this setting off.

The e-safety officer delivers yearly parental e-safety update evenings. Parents are given information about how they can monitor their child's activities on their devices and how to open up conversations with their child about their online activities which are often difficult to track outside of the home Wi-Fi.

The school has a browser extension 'Ripple' enabled. This is an interceptive tool designed to present a visual prompt when a person searches for harmful keywords or phrases relating to the topic of self-harm or suicide. These phrases include any words or terminology which have been identified as displaying potentially damaging online content. It works alongside Smoothwall, IMPERO and SENSO.

Section 4:

Roles and Responsibilities

We will ensure that designated staff in school have designated responsibilities with regard to e-safety. These roles and responsibilities are detailed below.

E-Safety Coordinator:

Our school's **e-Safety Coordinator** is Samantha Howes. He has responsibility for:

- Developing an e-safe culture under the direction of the leadership team.
- Acting as a key point of contact on all e-safety issues.
- Raising awareness and understanding of e-safety to all stakeholders, including parents and carers.
- Embedding e-safety in staff training, continuing professional development and across the curriculum and learning activities.

- Maintaining an e-safety incident log and reporting on issues.
- Understanding the relevant legislation.
- Liaising with the local authority and other agencies as appropriate.
- Reviewing and updating e-safety policies and procedures regularly.

- Receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
 - content
 - contact
 - conduct
 - commerce

CEOP Ambassador:

Our **Child Exploitation and Online Protection (CEOP) ambassador** is Samantha Howes. CEOP is a Government law enforcement agency focusing on child protection, particularly online protection. Samantha Howes has completed the CEOP 'Online Child Sexual Abuse' Course and 'CEOP Education Ambassador Training' to provide the knowledge, skills and resources to be the e-safety lead within Range High School and to be able to provide appropriate training and information relating to online child sexual abuse. Her main responsibility is therefore to help and advise members of staff regarding how to support young people and help prevent online child sexual abuse. She also has responsibility for:

- Attending training sessions and refresher courses (especially those held by CEOP) and other professional body providers.
- Ensuring e-safety is included in Computer Science schemes of work and updated regularly to take into account new technologies as they are developed and to liaise with the PHSE Co-ordinator to ensure continuity.

All Staff:

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials. Staff should report any concerns to the e-safety coordinator (Samantha Howes) immediately.

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to (insert relevant person) for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are 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 lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.

- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Section 5:

E-Safety in the Curriculum

We believe it is essential for e-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote e-Safety.

- The school has a framework for teaching internet skills in Computer Science/ PSHE lessons. Our CEOP ambassador (Samantha Howes) updates and maintains a range of teaching resources to promote e-safety.
- Online Safety will be taught discretely in Computer Science lessons across Years 7-9. This will largely be **factual** and will allow students to develop their **knowledge** of online safety issues.
- Online Safety will also be covered across Years 7-13 in PSHE.
- The content is phased and is relevant to specific year groups. The themes are as follows:
 - Year 7 – **Aggression** (bullying, harassment, stalking, violence, hateful content)
 - Year 8 – **Commercial** (Tracking, harvesting personal information, phishing, spam, spim, illegal downloading, hacking, viruses, gambling, scams)
 - Year 9-10 – **Sexual** (meeting strangers, grooming, pornographic/unwelcome sexual content, sexting, laws).
- Educating pupils on the dangers of technologies that maybe encountered outside school is also done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people’s information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.
- The curriculum incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week through assemblies tutorial sessions

Section 6:

Support from Parents/Carers

We will offer the following strategies through calendared ‘E-Safety Update’ evenings and our website:

- Don’t wait for something to happen before you act. Make sure your child understands how to use these technologies safely and knows about the risks and consequences of misusing them

- Make sure they know what to do if they or someone they know are being bullied online
- Encourage your child to talk to you if they have any problems. If they do have a problem, contact the school, the mobile network or the Internet Service Provider (ISP) to do something about it
- Parental control software can limit who your child sends emails to and who he or she receives them from. It can also block access to websites that are not age appropriate
- Make it your business to know what your child is doing online and who your child's online friends are
- It is important that parents and carers ensure that their children are engaged in safe and responsible online behaviour. Some suggestions for parents to stay involved are:
 - Have agreed family guidelines to check on your child's internet use and promote good 'device hygiene.'
 - Discuss the kinds of Internet activities your child enjoys
 - Be up front with your child that you will periodically investigate the files on the computer, the browser history files, and your child's public online activities
 - Search for your child's name online, look at his or her profiles and postings on teen community sites, review web pages or blogs
 - Tell your child that you may review his or her private communication activities if you have reason to believe you will find unsafe or irresponsible behaviour
 - Watch out for secretive behaviour as you approach the computer, such as rapidly switching screens, and for attempts to hide online behaviour, such as an empty history file
- We provide more detailed advice on our website

We believe that it is essential for parents/ carers to be fully involved with promoting e-Safety both in and outside of school and also to be aware of their responsibilities. We consult and discuss e-Safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website, school social networking accounts)
- The school disseminates information to parents relating to e-Safety where appropriate in the form of:
 - Posters
 - Website/VLE
 - Newsletter items
 - Parent Mail

Section 7

Reporting and Responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies (School VLE and website, CEOP Report Abuse, Report Remove & Report Hurtful Content).
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.

- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures, this may include (see below flowchart):
 - Non-consensual images
 - Self-generated images
 - Terrorism/extremism
 - Hate crime/ Abuse
 - Fraud and extortion
 - Harassment/stalking
 - Child Sexual Abuse Material (CSAM)
 - Child Sexual Exploitation Grooming
 - Extreme Pornography
 - Sale of illegal materials/substances
 - Cyber or hacking offences under the Computer Misuse Act
 - Copyright theft or piracy
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Trustees and the local authority / MAT
- where there is no suspected illegal activity, devices may be checked using the following procedures:
 - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
 - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
 - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
 - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
 - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - internal response or discipline procedures
 - involvement by local authority / MAT (as relevant)
 - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged with Safeguard and over email (itservices@range.sefton.sch.uk)
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
 - the Online Safety Lead for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
 - staff, through regular briefings
 - learners, through assemblies/lessons
 - parents/carers, through newsletters, school social media, website
 - trustees, through regular safeguarding updates
 - local authority/external agencies, as relevant

Reporting Harmful Content

The school operates a three staged process for both staff and students that should be followed to remove unwanted content that has been posted about them online.

- **Step 1** – Ask the person who posted the content to remove it (if possible).
- **Step 2** – Report the post to the platform (if possible) and wait 48 hours.
- **Step 3** – Make a report to reportharmfulcontent.com/report. This is an independent organisation that will work with you to have the content removed. A link to this website has been placed on the school website and on the VLE under the 'online safety' tab.

Reporting Sexual Abuse

- If a student does not feel comfortable disclosing sexual abuse to an adult, they can make a report to CEOP. www.ceop.police.uk/Safety-Centre. A link to this website has been placed on the school website and on the VLE under the 'online safety' tab.
- CEOP is an organisation that aims to keep children safe from sexual abuse. Students can make a report to CEOP if someone...
 - has asked them to send nude images
 - is asking them to live video chat to do things they don't want to do
 - is putting pressure on them to meet face-to-face
 - is talking to them about sex which makes them feel uncomfortable
 - is putting pressure on them to do things they don't want to do
 - is threatening them after they have sent them a nude image
- Once a report has been submitted:
 - It will be read by a child protection advisor
 - A child protection advisor will contact them by phone or email as soon as they can
 - The child protection advisor may need to talk to other adults about the report

Report Remove

Report Remove works with the Internet Watch Foundation (IWF) and Yoti to help to remove any sexual image or video of young people that's online. A link to this website has been placed on the school website and on the VLE under the 'online safety' tab. Young people will;

- Choose their age range
- Create a Childline account so they can send updates on the report
- Report the image or video to the Internet Watch Foundation (IWF)
- Talk to a Childline counsellor if the young person wants any extra support, or access support on the Childline website
- Check their Childline locker a few days after their report to see if they need to add any more information and to see updates on your report
- Report any issues with this process by sending an email from their Childline locker with the subject 'Report Remove' and as much information about the problem as they can.

Text/Video Messaging:

- You can turn off incoming messages for a couple of days
- If bullying persists you can change your phone number (ask your mobile service provider)
- Do not reply to abusive or worrying text or video messages - your mobile service provider will have a number for you to ring or text to report phone bullying. Visit their website for details

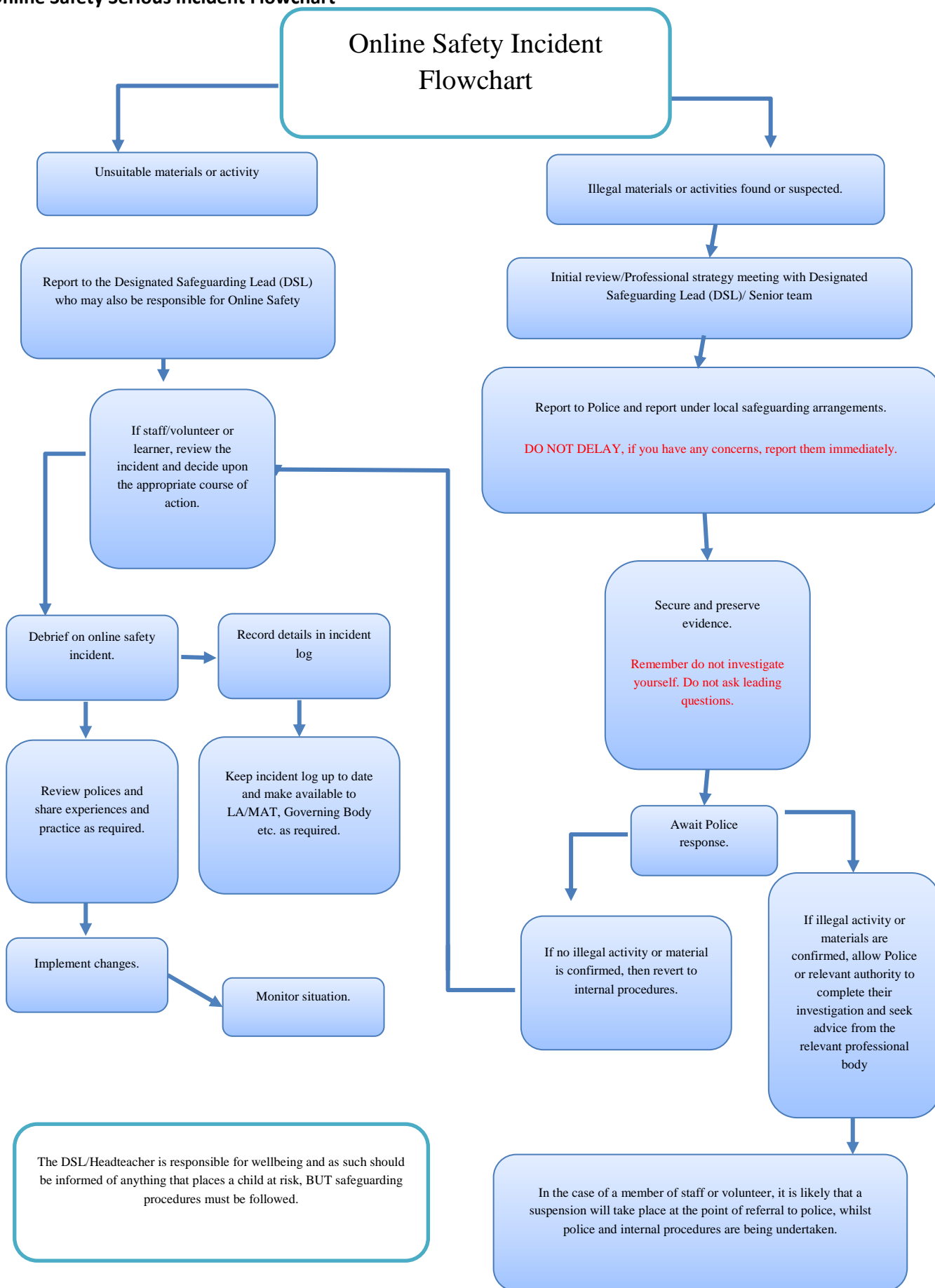
Email:

- Never reply to unpleasant or unwanted emails
- Don't accept emails or open files from people you do not know
- Ask an adult to contact the sender's ISP by writing `abuse@` and then the host, e.g. abuse@hotmail.com.

Chat Room & Instant Messaging

- Never give out your name, address, phone number, school name or password online. It's a good idea to use a nickname.
- Do not give out photos of yourself either
- Do not accept emails or open files from people you do not know
- Remember it might not just be people your own age in a chat room / instant messaging room
- End the conversation if you feel uncomfortable
- Tell your parents or carers if you feel uncomfortable or worried about anything that happens
- Think carefully about what you write and remember everything that you write can also be traced

Online Safety Serious Incident Flowchart



Section 8

How will complaints regarding e-safety be handled?

The school will take all reasonable precautions to ensure e-Safety. However, due to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview/counselling by tutor / Head of House / e-Safety Co-ordinator / Headteacher;
- Informing parents or carers;
- Removal of internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
- Referral to Social Care / Police

Any complaint about staff misuse or bullying or complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy or the Staff Disciplinary Policy.

Complaints related to child protection are dealt with in accordance with school / LSCB child protection procedures. Julie McGugan is the first port of contact for all child protection concerns.

Section 9

Reviewing our Policy

We will review our e-safety policy using the following measures:

- The number of incidents that are reported to staff over a given period
- Pupils' perceptions of the scale through periodic questionnaires and discussions with the Year and School Councils

We recognise that there may be times when parents feel that we have not dealt well with an incident of e-safety and we would ask that this be brought to the Headteacher's notice. If the Headteacher cannot resolve these concerns informally, parents can raise their concerns more formally through the school's Complaints Procedure. This involves contacting the clerk to the Trustees through school.

RELATED POLICIES

Our E-Safety policy links with and should be read in conjunction with the other sections of the Safeguarding Policy, and:

- Health & Safety Policy

Computer Network Acceptable Use Policy (AUP) for Students

Access to the school network is provided for you to carry out recognised schoolwork and extra-curricular activities, but only on the condition that you agree to follow this AUP.

Each time you log onto the computer network, you are shown a summary of this AUP. By clicking 'OK' and entering your username and password, you are agreeing to abide by this AUP.

We define our network as:

- using a physically wired computer
- accessing the network using a Wireless Access Point on a personal device
- accessing the school website and email
- accessing the VLE and Google Workspace (Google Classroom, Google Drive) Internally and Externally)

The following conditions also apply to those who use our network via our Wireless Access Points (WAPs). These are not for personal use.

General

- You are responsible for all use of your account on the school network. Never tell your password to anyone else or let them use your account. If you think someone has discovered your password or is using your account, tell a member of the IT staff immediately.
- Never use another person's account. You must not attempt to install any programs on a school computer or run them from removable media. You must not attempt to by-pass any security systems, modify any profile or install registry entries.
- You must only use a printer for school-related work and activities. Careless or deliberate wasting of paper will result in your printing facility being withdrawn. All printing use is monitored and may be checked at any time.
- Eating and drinking are strictly prohibited in any computer room.
- Always make sure that you have completely logged off the computer before leaving it unattended.
- Always leave the computer and the surroundings as you would like to find them.
- No computer equipment may ever be removed from its location or tampered with. Any such interference with school property will be reported to the Head of Computer Science, or if appropriate to the Head Teacher.
- 'Hacking' i.e. unauthorised access or use of personal information, contrary to the provisions of the General Data Protection Regulation (GDPR), is a serious offence. Intentional damage to computers, computer systems or computer networks, including unauthorised damage or interference to any files may be considered a criminal offence under the Computer Misuse Act 1990.
- You should be aware that the unauthorised copying of software, images or documents is contrary to the provisions of the Copyright, Designs & Patents Act 1988 and is not permitted.
- The installation, copying or transmitting of obscene material is not permitted and may be considered a criminal offence under the Obscene Publications Act 1959/1964. In addition, any material in your account which the school considers inappropriate (including music, video and computer game files) or offensive will be removed immediately without prior warning.
- All files stored on the network will be treated as school property, including e-mail. IT Services staff and Computer Science staff may look at files and communications at any time to ensure that the system is being used responsibly, especially if they have a reasonable suspicion that the system is being misused. You should not expect that your work and e-mails will always be private.
- You should only use your own personal devices (mobile phones/laptop etc.) in school if you have permission. You must understand that, if you do use your own devices in the school, you will follow the rules set out in this agreement, in the same way as if you were using school equipment.
- You should immediately report any damage or faults involving equipment or software; however this may have happened.

The Internet and E-mail

The Internet is provided for you to conduct genuine research and communicate with others. All the sites you visit are recorded and kept for at least 6 months. Remember that access is a privilege, not a right, and that access requires responsibility at all times.

- You must never send, display, access or try to access any obscene or offensive material. You must not use obscene or offensive language in e-mails. Remember that you are a representative of your school on a global public system - never swear, use vulgarities, or any other inappropriate language. Remember that the school has the right to read your e-mails.
- You must never harass, insult or attack others through electronic media. Within the school this is bullying and will be punished as such. Also, e-mail 'bombing' is a serious offence and will result in your suspension from the system. Remember that any e-mail you send can be traced. A recipient of an offensive e-mail from you may take legal action against you. You must not attempt to bypass internet and email restrictions using any method including the use of online proxy / firewall bypass sites.
- Never copy and make use of any material without giving credit to the author. Not only are you infringing copyright, but also you will be guilty of plagiarism. If you are a student in Key Stage 4 or 5 and are suspected of plagiarism as part of your coursework or Non-Exam Assessments (NEA) the relevant exam boards will be informed.
- In using school computers and the internet, you must be cautious of "stranger danger" and avoid disclosing personal information, including names, addresses, email addresses, telephone numbers, age, gender, educational details, and financial details. You should never arrange offline meetings with individuals you've met online without doing so in a public place and bringing along a responsible adult. If you encounter any unpleasant or inappropriate material or messages online that make you feel uncomfortable, you must promptly report them.
- Check with a member of the Computer Science staff before opening unidentified e-mail attachments or completing questionnaires or subscription forms.
- A log of all emails sent, received and forwarded is kept forever by Gmail, even if you delete them from your own mailbox. All files stored in your google drive account are kept forever by Google, even if you delete them.

Games

With the exception of educational games expressly permitted by a member of staff, games may never be played from any pupil's account, from removable media or over the internet. Never attempt to download any games or executable programs from the internet without the express permission of a member of the IT Services team.

Sanctions

The school uses IMPERO/SENSO software to monitor your activities. The software will take photographs of your screen if it determines that you have breached the conditions outlined in this AUP. Any infringement of the AUP will be reported to the CAL of Computer Science and the Network Manager. Punishments will vary dependant on the severity of the infringement, but may include:

- A detention
- A temporary network/internet ban
- Your parents / carers / head of house being informed
- A permanent network/internet ban

For more serious offences, such as the transmission of offensive material or 'hacking', the Head Teacher, and your parents will be informed. Note that if a criminal offence appears to have been committed, the school will refer the matter to the police.

Note that this AUP may be updated from time to time. The latest AUP can be found on the school website at <http://www.range.sefton.sch.uk> .

Appendix B

Range High Acceptable Use Policy (AUP) for Staff

Computer Network Acceptable Use Policy (AUP) for Staff

Access to the school network is provided for you to carry out recognised schoolwork, but only on the condition that you agree to follow this AUP.

Important Note: The school has a cyber-security insurance policy in place. This will compensate the school if a cyber-attack has taken place and the school is not at fault. The school would not be insured if a cyber-attack took place due to staff not following this AUP.

Each time you log onto the computer network, you are shown a summary of this AUP. By clicking 'OK' and entering your username and password, you are agreeing to abide by this AUP.

We define our network as:

- using a physically wired computer
- accessing the network using a Wireless Access Point on a personal device
- accessing the school website and email
- accessing the VLE, Google Workspace (Google Classroom, Google Drive), SIMS and ClassCharts (internally and externally)

The following conditions also apply to those who use our network via our Wireless Access Points (WAPs). These are not for personal use.

You are allowed to use the school network for personal purposes as long as that usage

1. Is not illegal
2. Is compatible with the school's safeguarding policy
3. Is compatible with the Staff Code of Conduct
4. Is on your own device or in a private staff area
5. Is not in view of pupils
6. Is not in directed time

Ask a member of SLT for guidance if you are unsure.

This AUP forms part of our overall Staff Code of Conduct.

General

- You are responsible for all use of your account on the school network. Never tell your password to anyone else or let them use your account. If you think someone has discovered your password or is using your account, tell a member of the IT services immediately.
- Never use another person's account. You must not attempt to install any programs on a school computer or run them from removable media. You must not attempt to by-pass any security systems, modify any profile or install registry entries.
- Images of pupils and/or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of Julie McGugan.
- You have responsibility for checking all ICT (especially online based) resources (e.g. clips from YouTube) before they are used with pupils to ensure that the resources are appropriate and will not cause offence to any pupils or other members of staff.
- You have responsibility for checking resources that store student details (e.g. senecalearning.com, quizz.com) to ensure all data transmission is encrypted and that the website keeps students details safe and secure (e.g. checking websites use HTTPS).

- You must only use a printer for school-related work and activities. Careless or deliberate wasting of paper will result in your printing facility being withdrawn. All printing use is monitored and may be checked at any time.
- Always make sure that you have completely logged off the computer before leaving it unattended.
- Always leave the computer and the surroundings as you would like to find them.

- No computer equipment may ever be removed from its location or tampered with. Any such interference with school property will be reported to the Head of Computer Science, or if appropriate to the Head Teacher.
- 'Hacking' i.e. unauthorised access or use of personal information, contrary to the provisions of the General Data Protection Regulation (GDPR), is a serious offence. Intentional damage to computers, computer systems or computer networks, including unauthorised damage or interference to any files may be considered a criminal offence under the Computer Misuse Act 1990.
- You should be aware that the unauthorised copying of software, images or documents is contrary to the provisions of the Copyright, Designs & Patents Act 1988 and is not permitted.
- The installation, copying or transmitting of obscene material is not permitted and may be considered a criminal offence under the Obscene Publications Act 1959/1964. In addition, any material in your account which the school considers inappropriate (including music, video or game files) or offensive will be removed immediately without prior warning.

By agreeing to the Staff AUP you undertake to abide by Data Protection legislation (GDPR) and should familiarise yourself with the school's Data Protection Policy if you use school data away from the school site or on a device which does not belong to the school. The school has assessed the related benefits and disadvantages of requiring double encryption log-ins and decided that the disadvantages currently outweigh the benefits. The school will therefore not require double authentication log-ins. You undertake to make all efforts to protect school data by:

1. Using encryption on any portable data storage devices ("memory sticks") used to hold school data. You must ask the IT technicians to check encryption is enabled on any of your own devices, or use a device provided by the school which will have encryption.
2. Ensuring any of your own tablets or smartphones which are permanently logged into the school network are password protected and have a 'locate and wipe' facility which can be used if they are lost or stolen. Please see the IT technicians to check the status of your device. If your device does not have this facility you must log out of the school system after each episode of use.
3. Ensuring that you log out of the school network if using devices at home to prevent those who are not Range High School employees from accessing any data.
4. Signing the SIMS Code of Conduct if you wish to be allowed to use SIMS at home.
5. Not showing student data on a whiteboard such as names, assessment scores etc.

Shared Drive/VLE/Google Workspace

- All files held on the network or VLE will be treated as school property, including e-mail. IT services staff may look at files and communications to ensure that the system is being used responsibly. You should not expect that your work and e-mails will always be private (with regards to Freedom of Information; Safeguarding & Disciplinary matters).
- Sensitivity should be taken when putting files onto the shared drive and inappropriate or offensive materials should not be placed onto the shared drive or the VLE.
- You must not tamper with files belonging to other members of staff such as deleting, moving or editing files that you are not authorised to.

Passwords

- All passwords should be complex so that they are not easy to guess. Strong passwords include:
 - Eight characters
 - Lower and upper case letters
 - Letters and numbers
 - Special characters (e.g. # ! *)

- You must change your passwords frequently (every three months minimum). This includes the password you use to access school network and your SIMS passwords. You should not write passwords down or tell people your passwords.
- You must use a different password for each account or software (e.g. Network and SIMS). You must also use different passwords for your personal and school accounts.
- Don't use passwords that you have previously used before.

The Internet and E-mail

The Internet is provided for you to carryout your day-to-day roles. All websites you visit are recorded and kept on record.

- You must never send, display, access or try to access any obscene or offensive material. You must not use obscene or offensive language in e-mails. Remember that you are a representative of your school on a global public system - never swear, use vulgarities, or any other inappropriate language. Remember that the school has the right to read your e-mails under certain conditions. Your emails will not be routinely monitored. However the SLT reserve the right to look at staff emails if they have reasonable suspicion that the system has been misused, or a safeguarding issue has arisen. Freedom of Information requests may result in your e-mails being read by the parents of pupils. Never write something in an e-mail which you would not like to be read by them.
- You must never harass, insult or attack others through electronic media. Within the school this is bullying and will be punished as such. Also, e-mail 'bombing' is an offence and will result in your suspension from the system. Remember that any e-mail you send can be traced. A recipient of an offensive e-mail from you may take legal action against you. You must not attempt to bypass internet and email restrictions using any method including the use of online proxy / firewall bypass sites.
- Never copy and make use of any material without giving credit to the author. Not only are you infringing copyright, but also you will be guilty of plagiarism.
- Never reveal any personal information, the home address or personal phone numbers of yourself or other people.
- A warning will usually be displayed when you are potentially accessing a harmful email. If this is the case, you should be very cautious about replying, clicking any links or downloading any attachments.
- A summary of what does, and does not constitute responsible internet use is displayed in all IT rooms. Use of the school system is an acknowledgement of acceptance of these guidelines.
- Never attempt to download any games or executable programs from the internet without the express permission of a member of the IT Services team.
- When using SIMS ensure pupil data remains confidential.
- A log of all emails sent, received and forwarded is kept forever by Gmail, even if you delete them from your own mailbox. All files stored on the VLE or in your google drive account are kept forever by Google, even if you delete them.
- Staff should make every effort to limit the sending of emails to within normal working hours, and in the event of sending emails outside of these hours, ensure they are scheduled to be sent during the next working day.

Sanctions

Any infringement of the AUP will be reported to the Head of Computer Science and the Network Manager. Punishments will vary dependant on the severity of the infringement.

For more serious offences, such as the transmission of offensive material or 'hacking', the Headteacher will be informed. Note that if a criminal offence appears to have been committed, the school will refer the matter to the police.

Note that this AUP may be updated from time to time. The latest AUP can be found on the VLE.

Home access to SIMS Protocol

Information held on SIMS about pupils is sensitive and confidential. Colleagues must make all efforts to ensure this data remains confidential. **Failure to do so may result in disciplinary action.** This contract serves as a formal record that colleagues who use SIMS at home are conscious of this obligation.

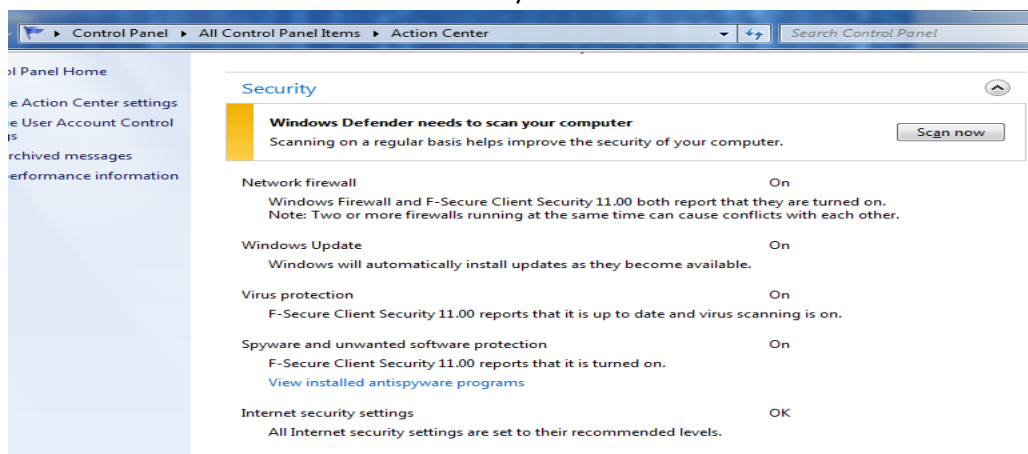
In order for you to have access to SIMS from home you must sign and return this document to the school’s Network Manager before permissions can be granted. You will receive an email once access has been authorised.

By signing this protocol you agree to all the conditions below and take all reasonable responsibility for ensuring there is no unauthorised access via your login route or username and password. Failure to do so could not only jeopardise the security of the school’s information management system but could also lead to disciplinary action being instigated.

At present only computers that use the Windows operating system can access SIMS from home. If you have an Apple Mac machine and would like to investigate further how you can gain access please speak to the Network Manager.

Conditions of use

1. Ensure that your computer has working Anti-Virus and firewall software installed, and that your computer is fully upto date with the latest Windows Updates. To do this go to the “Action Center” (found in Control Panel) and check the status under the security tab: -



2. Anything in red requires your attention.
3. **Do not use** this connection in an unsecure / public place such as an Internet Café or via Hotel / public Wifi etc. If you are using your home wifi to connect, make sure it is suitably secured with a password (not the default) and encryption enabled.
4. **Never** share your curriculum and SIMS password and ensure that they are both suitably complex.
5. **Do not** leave your computer unattended while using this connection.
6. **Do not** copy any information obtained from SIMS to your personal computer or personal storage device.
7. Once you have finished using SIMS ensure that you close it down and then click the **“Sign out”** link.

Contact the IT Technicians if you have any issues with the above requirements.

Signed: _____ Email: _____
Name: _____ Date: _____