# MAGHULL HIGH SCHOOL

# Online Safety Policy

## Contents

Page:

## Mission Statement

The online safety policy covers the safe use of Information Communication Technology (ICT) both inside of school (e.g. by using the computer network) and outside of school (e.g. accessing the VLE, school emails or the school website from home).

The policy will be reviewed at, or prior to, the start of each academic year and promptly in the following instances:

- Serious and/or frequent breaches of the Acceptable Internet Use Policy or in the light of e-safety incidents.
- New guidance by government/local authority/safeguarding authorities.
- Significant changes in technology as used by the school or students in the wider community.
- E-safety incidents in the community or local schools which might impact on the school community.
- Advice from the police and/or local safeguarding children partners.

We at Maghull 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 students with the skills to access life-long learning and employment.

We also recognise that such technology can be misused and as such, we acknowledge our responsibility to educate our students and staff about online 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. We will educate our students, staff and families about possible misuse and will provide education, infrastructure and processes which support safe use of a variety of technologies. We will designate specific roles and responsibilities and will provide a discrete Computing curriculum which addresses these issues. We will engage the support of families in this work and will have a defined complaints procedure for online safety. We will require all users to agree to Computer Network Codes of Conduct (see Appendices A and B.

## Definitions of Misuse

- Text message bullying involves sending unwelcome texts that are threatening or cause discomfort
- Picture/video-clip bullying via mobile phone cameras is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks
- Phone call bullying via mobile phone uses 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

- Email bullying uses 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 children or young people 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. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyberbullying

**School Social Media**

The school uses social media eg Twitter and Facebook as a form of communication with our stakeholders and the wider community. Any inappropriate comments or activity by parents or other persons will be dealt with in the same manner as if it was face-to-face. Any inappropriate activity by members of staff will be dealt with in accordance with the staff code of conduct. Only photographs or video footage of those students for whom we have permission will be shared on the school social media accounts.

The DSL has the overview and responsibility for the school social media accounts.

**Safe Use of Technology**

We will ensure appropriate filters and monitoring systems are in place across the school and will educate our students, staff and families to use the following technologies appropriately in the following manner:

**Email:**

- The school gives all 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 students, parents or conduct any school business using personal e-mail addresses
- Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- Students 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

- Students are introduced to e-mail as part of the Computing schemes of work in year seven and continue to use email to submit work throughout all key stages
- However staff access school e-mail, (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

**Internet Access:**

- The school has students who will have supervised access to Internet resources (where reasonable) through the school's wired and wireless technology
- Staff will preview any recommended sites before use
- 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, some use of mobile phones is allowed in coding and cyber security clubs and Sixth Form

**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.

- The school endeavours to deny access to social networking sites to students within school
- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Students 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 students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals
- Students are encouraged to be wary about publishing specific and detailed private thoughts online
- Our students are asked to report any incidents of bullying to the school

**Roles and Responsibilities**

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

Online Safety Coordinator:  Mr M Kay (Deputy Headteacher)

Designated Safeguarding Lead:  Mrs M Bennett (Senior Assistant Headteacher)

Safeguarding Governor:  Mrs J McDowall

They have responsibility for:

- Developing an 'e-safe' culture under the direction of the leadership team
- Acting as a key point of contact on all online safety issues
- Raising awareness and understanding of online safety to all stakeholders, including parents and carers
- Embedding online safety in staff training, continuing professional development and across the curriculum and learning activities
- Understanding the relevant legislation
- Liaising with the local authority and other agencies as appropriate
- Reviewing and updating online safety policies and procedures regularly

Appropriate network filters and monitoring systems are in place.  An online safety incident log (filtering of 'key terms' within email and search platforms for all staff and students) will be maintained by the network manager and a review of the reporting system will take place monthly.  As well as this, half termly Safeguarding Team meetings led by the DSL review online safety.

All staff

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

ICT support staff & external contractors

Internal ICT support staff and technicians are responsible for:

- Maintaining the school's networking, IT infrastructure and hardware.
- Keeping up to date with current thinking and trends in IT security.
- Ensuring that the school system, particularly file-sharing and access to the Internet, is secure.

- Taking all reasonable steps to ensure that systems are not open to abuse or unauthorised external access, with particular regard to external logins and wireless networking.
- Maintaining and enforcing the school's password policy and monitoring and maintaining the Internet filtering.
- Ensuring external contractors, such as VLE providers, website designers/hosts/maintenance contractors, are made aware of, and comply with, the school's e-safety policy.
- Completing DBS checks where contractors have access to sensitive school information and material covered by GDPR.

**Online safety in the Curriculum**

Online safety - The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material;

- contact: being subjected to harmful online interaction with other users;

- conduct: personal online behaviour that increases the likelihood of, or causes, harm.

We believe it is essential for online safety guidance to be given to the students on a regular and meaningful basis. Online safety is embedded within our curriculum and we continually look for new opportunities to promote online safety. The school has a strong culture of online safety.

- The school has a framework for teaching internet skills in Computing/ PD lessons. There is a range of teaching resources to promote online safety across the school
- Annual safeguarding assemblies whole school address online safety
- Safer Internet Week is promoted annually with a week of assemblies and associated lessons
- Online Safety will be taught discretely in Computing lessons in KS3 and in option subjects at KS4 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 PD and across the curriculum. This will largely be discussion based which will allow students to discuss the impacts & consequences of their actions online
- Educating students on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the online safety curriculum
- Students 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
- Students are taught about copyright and respecting other people's information and images through discussion, modelling and activities
- Students are aware of the impact of online bullying and know how to seek help if they are affected by any form of online bullying.
- Students 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

There is a wealth of information available to support schools to keep children safe online. The following is not exhaustive but provides a useful starting point:

- www.thinkuknow.co.uk
- www.parentzone.org.uk
- www.disrespectnobody.co.uk
- www.saferinternet.org.uk
- www.internetmatters.org
- www.childnet.com/cyberbullying-guidance
- www.pshe-association.org.uk
- educateagainsthate.com
- www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

**Support from Parents/Carers**

We recommend the following strategies through school 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 cyberbullied
- Encourage your child to talk to you if they have any problems with Cyberbullying. 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 some chat rooms
- 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:
- Keep the computer in a public place in the house. Periodically check on what your child is doing
- 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 believe that it is essential for parents/ carers to be fully involved with promoting online safety both in and outside of school and also to be aware of their responsibilities. We consult and discuss online 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
- The school disseminates information to parents relating to online safety where appropriate in the form of:
- o Posters
- o Website
- o Newsletter items

**Responsibilities of Students**

Students could adopt one or more of the following strategies. These will be outlined in online safety lessons in the Computing curriculum.

- If you are being bullied, remember bullying is never your fault. It can be stopped and it can usually be traced. Don't ignore the bullying. Tell someone you trust, such as a teacher or parent, or call an advice line. Try to keep calm. If you are frightened, try to show it as little as possible. Don't get angry, it will only make the person bullying you more likely to continue. There is plenty of online advice on how to react to cyberbullying. For example, www.kidscape.org.uk and www.wiredsafety.org have some useful tips.

**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.

**Web:**

- If the bullying is on the school website, tell a teacher or parent, just as you would if the bullying was face-to-face

**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
- Stick to public areas in chat rooms and get out if you feel uncomfortable
- Tell your parents or carers if you feel uncomfortable or worried about anything that happens in a chat room
- Think carefully about what you write - don't leave yourself open to bullying

**Responsibilities of Other Users**

School visitors, wider school community stakeholders and external contractors should be expected to agree to a visitor's AUP document or a tailored AUP document specific to their level of access and usage.

External users with significant access to school systems which include sensitive information or information held securely under the General Data Protection Regulations should be DBS checked. This includes external contractors who might maintain the school domain name and web hosting – which would facilitate access to cloud file storage, website documents and email.

**How will complaints regarding online safety be handled?**

The school will take all reasonable precautions to ensure online 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. Neither the School nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

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

- Interview/counselling by tutor / Pastoral Manager / Online 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 LA / Police

Any complaint about staff misuse or bullying or complaints of online abuse are dealt with in accordance with our Anti-Bullying Policy.

Complaints related to child protection are dealt with in accordance with school / LSCB child protection procedures. Designated Safeguarding Lead (Mrs M Bennett) is the first point of contact for all child protection concerns.

**Online Safety in Practice**

The school will ensure that:

- School computer systems are fit for purpose and customised to ensure e-safety while meeting teaching and learning requirements.
- It is possible to trace every login, data transaction, or other activity to a particular user.
- Servers, network switches, cloud-based systems, hubs, Cat5 or Fibre Optic cabling, wireless transmitters, bridges, access points and other physical architecture should be secured to prevent unauthorised or untraceable network access.
- Risk assessments will be made of any new equipment, technologies or systems.
- Regular audits of systems are carried out.
- The school's Internet service is provided by a fully accredited ISP.
- Filtering and monitoring is in place and any filtering incidents are examined to prevent a reoccurrence.
- The school has in place a password policy that is fit for purpose with students and staff encouraged to change passwords regularly.
- The school has protocols in place to meet the requirements of GDPR as defined by the Information Commissioner's Office.
- When disposing of equipment, the school ensures all data is wiped irretrievably.
- Policies are in place around the taking and sharing of images of children.

- The school will make it clear to students and staff which online and network activities are appropriate and which are not.

**Reviewing our Policy**

We will review our online safety policy using the following measures:

- The number of incidents that are reported to staff over a given period
- Students' 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 online safety and we would ask that this be brought to the Head Teacher's notice. If the Head Teacher 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 Governors through school.

RELATED POLICIES

Our Online safety policy links with, and should be read in conjunction with, the other sections of the Child Protection and Safeguarding Policy, Health & Safety Policy and Home School Agreement.

## Appendix A

### Maghull High School Computer Network Code of Conduct for Students

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, access the VLE (internally/externally) and SIMs from home

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

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 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 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 IT room.

Always make sure that you have completely logged off the computer before leaving it unattended. Do not use the reset button as a means of switching off.

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 Network Manager, or if appropriate to the Head Teacher.

'Hacking' i.e. unauthorised access or use of personal information, contrary to the provisions of 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 Voyeurism Act 2019. In addition, any material in your account which the school considers inappropriate (including music and video files) or offensive will be removed immediately without prior warning.

All files held on the network 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.

**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. 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, denial of service 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.

Never reveal any personal information, the home address or personal phone numbers of yourself or other people.

Check with a member of the Network Manager before opening unidentified e-mail attachments or completing questionnaires or subscription forms.

**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 Computer Science Department.

**Sanctions**

Any infringement of the Code of Conduct will be reported to 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 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 Code of Conduct may be updated from time to time. The latest Code of Conduct can be found on the school website at www.maghullhigh.com

**Appendix B**

**Maghull High School Computer Network Code of Conduct for Staff**

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
- accessing the VLE (internally/externally) and SIMs from home

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

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 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 the Network Manager 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 students 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 The Designated Safeguarding Lead (Mrs Bennett). Report of all data held on SIMS.

You have responsibility for checking all ICT (especially those that are online based) resources (e.g. clips from YouTube) before they are used with students to ensure that the resources are appropriate and will not cause offence to any students or other members of staff.

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. Do not use the reset button as a means of switching off.

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 IT, or if appropriate to the Head Teacher.

'Hacking' i.e. unauthorised access or use of personal information, contrary to the provisions of the 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 Communications Act 2003 and is not permitted.

The installation, copying or transmitting of obscene material is not permitted and may be considered a criminal offence under the Voyeurism Act 2019.

In addition, any material in your account which the school considers inappropriate (including music and video files) or offensive will be removed immediately without prior warning.

**Shared Drive/VLE**

All files held on the network will be treated as school property, including e-mail. The Network Manager or Headteacher 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.

**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. 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, denial of service 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.

Never reveal any personal information, the home address or personal phone numbers of yourself or other people.

Check with a member of the Computer Science staff before opening unidentified e-mail attachments or completing questionnaires or subscription forms.

Never attempt to download any games or executable programs from the Internet without the express permission of a member of the Computer Science department.

When using SIMS ensure pupil data remains confidential

**Sanctions**

Any infringement of the Code of Conduct may be reported to the Headteacher. Consequences 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 Code of Conduct may be updated from time to time and distributed to staff.

## APPENDIX C

## 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.

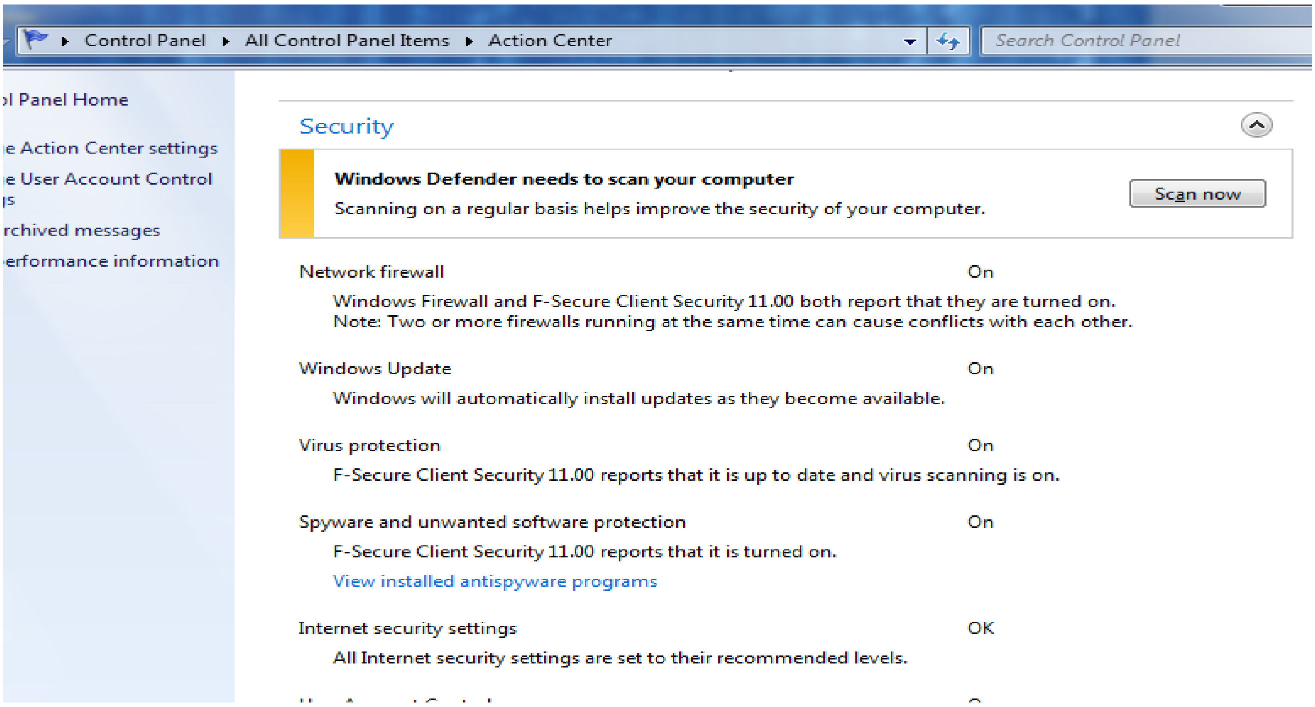
In order for you to have access to SIMS from home you must sign and return this document to the school's Network Manager before permissions can be granted. You will receive an email once access has been authorised.

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.

Computers that can use the Windows or Apple Mac operating system can access SIMS from home. Detailed instructions are available from 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 up to 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: -



Security

**Windows Defender needs to scan your computer**

Scanning on a regular basis helps improve the security of your computer.

Network firewall On

Windows Firewall and F-Secure Client Security 11.00 both report that they are turned on.
Note: Two or more firewalls running at the same time can cause conflicts with each other.

Windows Update On

Windows will automatically install updates as they become available.

Virus protection On

F-Secure Client Security 11.00 reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On

F-Secure Client Security 11.00 reports that it is turned on.

View installed antispyware programs

Internet security settings OK

All Internet security settings are set to their recommended levels.

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. **Do not use** easily guessable dictionary words and make sure that your SIMS password is different to your curriculum password.

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 Network Manager if you have any issues with the above requirements.

**Signed:** ______________________ **Email:** ______________________

**Name:** ______________________ **Date:** ______________________