RAINHILL HIGH SCHOOL

E SAFETY

LFC ACADEMY EDUCATION CENTRE
LFC WOMEN

FOWLER

LIPA 4:19 ASSOCIATE ACADEMY

DUAL CAREER ACCREDITED tass+

DCS Centre of Excellence

ARTS COUNCIL ENGLAND
Artsmark Platinum Award
Awarded by Arts Council England

St Helens Chamber

SCHOOLS IN PARTNERSHIP
STEPHENSON MULTI ACADEMY TRUST

E Safety Policy

Approved by :	**Local Governing Body**
Signed:	**Josie Thorogood** **Angela Afflick** **Headteacher** **Chair of PDBW**
Approval Date:	**3 July 2019**
Review Date:	**July 2022**

CONTENTS

1. Rationale

The use of 'Information and Communication Technologies (ICT)' has great benefits for the development of students' learning and the administration and governance of a school. With these advantages, however, come insignificant risks, including:

1.1 sexual exploitation
1.2 identity theft
1.3 spam
1.4 'cyber' bullying
1.5 Viruses

It is the aim of this policy to minimise these risks for

1.6 students
1.7 staff and others involved with the daily activities of the school.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and students (Appendix 1), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/student discipline (including the anti-bullying) policy and PSHE.

2. What is 'Unsafe' Use of ICT

This policy is concerned with significantly unsafe use of ICT, not minor infringements. Just as safe use of ICT is commonly known as e-safety, unsafe use of ICT is an e-safety incident. E-safety incident:

2.1 uses some form of technology
2.2 causes or could have caused significant offence, harm or distress
2.3 may or may not be deliberate
2.4 may not have occurred within school or on school equipment.

Examples of e-safety incidents (not exclusive) include:

2.5 a student or member of staff viewing pornography on a school computer
2.6 a student bullying someone from another school with text messages
2.7 a student bullying a fellow student using instant messaging services such as MSN from home
2.8 a student placing distressing posts about a member of the school community on social networking sites like Facebook
2.9 a student publishing their own address details on the internet
2.10 a student publishing revealing images of her or himself on a social networking site
2.11 a student sharing a phone video of a member of staff in a lesson with other students
2.12 a member of staff suspecting a student of being groomed by a paedophile through their use of internet chat services
2.13 a student modifying a photo of a member of staff and distributing it leading to offence

3. Staff Responsibilities

3.1 e-Safety Coordinator

The school will identify an 'e-Safety Coordinator'; all members of the school community will be made aware of who holds this post. It is the role of the e-Safety Coordinator to:

3.1(a) keep abreast of current issues and guidance through organisations such as St Helens & Knowsley Safeguarding Board/ LA, CEOP (Child Exploitation and Online Protection) and Childnet

3.1(b) support staff in handling incidents

3.1(c) support education of students and staff in the safe use of ICT

3.2 Network Services Manager

Maintain services in support of the safe use of ICT. Typically to include;

3.2(a) internet and email filtering and logging

3.2(b) classroom management tools to monitor ICT use

3.2(c) network access logging

3.2(d) appropriate level of network security against malicious use

3.3 Other staff

3.3(a) know what is safe use of ICT

3.3(b) model safe use of ICT within the school community and beyond

3.3(c) be alert to unsafe use of ICT, by students & staff within school and beyond

3.3(d) manage & report incidents as appropriate

3.3(e) educate students where required by the curriculum

4. Student Responsibilities

4.1 Must adhere to the Acceptable Use Policy

4.2 Must report incidents as they occur through the most appropriate member of staff; current teacher, form tutor, YSM,YPL,KSPL or e-Safety Coordinator

5. Parent Responsibilities

5.1 Understand the Acceptable Use Policy and encourage their child to use ICT safely

5.2 Accept any sanctions that are applied when a student breaches the policy.

6. Education in Safe Use of ICT

6.1 Staff

6.1(a) All staff will be trained in the safe use of ICT both for themselves and for students they supervise.

6.1(b) This will be incorporated with the 3 year refresher training in Child Protection/Safeguarding.

6.1(c) New staff will receive information on the school's acceptable use policy as part of their induction.

The training will raise awareness of their individual responsibilities for the safeguarding of children within the context of e-Safety and will cover what to do in the event of misuse of technology by any member of the school community.

6.2 Students

6.2(a) The school will provide opportunities through the main areas of ICT, PHSE, Citizenship, discrete ESafety lesson, national focus days and assemblies. ESafety will and supported in other curriculum areas as appropriate and other more informal settings eg. Registration

6.2(b) The ICT curriculum will include relevant legislation such as Data Protection and intellectual property laws which may limit what they want to do but also serves to protect them

6.2(c) Students will be taught about copyright and respecting other people's information, images, and related topics

6.2(d) Students will be made aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying.

6.2(e) Students will be taught the dangers of releasing personal information through the use of social networking platforms and instant messaging / chat facilities. Where these technologies have good educational outcomes they will be available within our network services.

6.2(f) Students will also be made 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

7. Managing Technology

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All internal use of the Rainhill High School network is logged to allow any inappropriate use to be identified and followed up.

7.1 Infrastucture

Rainhill High School will monitor access and use of the school network including internet services, so activity is monitored and recorded. Email and internet activity can be monitored and explored further if required.

Rainhill High School will be aware of its responsibility when monitoring staff and student communication under current legislation and take into account:

7.1(a) Data Protection Act 1998,

7.1(b) The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000,

7.1(c) Regulation of Investigatory Powers Act 2000,

7.1(d) Human Rights Act 1998

The school will use management control tools for controlling and monitoring workstations.

7.2 Managing the Internet

All access to the internet will be monitored.

Staff will make every effort to preview sites before recommending them to students; it is recognised that internet sites are beyond the control of Rainhill High School.

All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

All users should make all reasonable attempts to observe copyright of materials from electronic resources.

Users must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience.

Users must not reveal personal information about members of the school community (including names) acquired through school life on any social networking site or blog without seeking the subject's permission. Information published on the internet prior to the adoption of this policy may remain where not causing an issue, however staff should declare any material in the public domain (to the Network Manager) which will be inspected for suitability.

Collaborative learning or blogging activity must be carried out only on school managed service e.g. an internal server or hosted solution. Further advice is available from the Network Manager.

8. Communication

Students, Parents, Staff and Governors are made aware of the School's e-Safety Policy through a variety of means:

8.1 The e-Safety policy will be introduced to the students at the start of each school year through ICT and PSHE

8.2 e-Safety messages will be embedded across the curriculum whenever the internet and/or related technologies are used including Assemblies and PHSE sessions

8.3 e-Safety posters will be prominently displayed

8.4 Parents will receive regular information regarding keeping their child safe (e safety information evenings, newsletters.

8.5 e-Safety updates will be displayed via the following methods;
8.4(a) school website
8.4(b) school learning platform
8.4(c) school screen savers

9. Specific E-Safety Issues

Further advice available http://www.itgovernance.co.uk/

9.1 Digital images & video

Digital images are easy to capture, reproduce and publish and, therefore, misuse. It is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

With the written consent of parents (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students. Staff should only take photographs or videos of students with the express permission of student and parent. This is normally obtained from parents on entry to the school and a list of the students whose parents have objected to this is kept by the Data Manager. It is preferred that school equipment is used for this, but in any case, images must be transferred within a reasonable time scale and solely to the school's network or hosted services controlled by the school and deleted from the original device.

Students must be advised when using their personal digital equipment, especially during field trips, that images and video should only be taken with the subjects' consent. Students should also be advised that complaints against this condition will be considered a serious breach of this policy and risk having the device confiscated until it can be inspected, in their presence, by the e-safety co-ordinator or a member of the Senior Leadership Team.

Permission to use images and video of all staff who work at the school is sought on induction and a copy is to be stored in the relevant personnel file.

9.2 Publishing Student's Images and Work

On a student's entry to the school, all Parents/carers are asked to give permission to use their student's work / photos in the following ways:

9.2(a) on the school web site
9.2(b) on the school's Learning Platform
9.2(c) in the school prospectus and other printed publications that the school may produce for promotional purposes
9.2(d) recorded/ transmitted on a video or webcam
9.2(e) in display material that may be used in the school's communal areas
9.2(f) in display material that may be used in external areas, ie exhibition promoting the school
9.2(g) general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/carers may withdraw permission, in writing, at any time. Consent has to be given by all interested parties in order for it to be deemed valid. Students' full names will not be published alongside their image by the school and vice versa. E-mail and postal addresses of students will not be published. Often, the press wishes to publish full names for members of teams. In these cases, the member of staff supervising will ensure that appropriate permission is sought. Before posting student work on the Internet, the member of staff responsible must check that permission has been given for work to be displayed.

9.3 Video Conferencing (includes Facetime)

9.3(a) All students are supervised by a member of staff when video conferencing.
9.3(b) Any conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences
9.3(c) No part of any video conference with end-points outside of the school is to be recorded in any medium without the written consent of those taking part

Additional points to consider:

9.3(d) Participants in conferences offered by 3rd party organisations may not be DBS checked
9.3(e) Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

For further information and guidance relating to Video Conferencing, please see http://www.thegrid.org.uk/learning/ict/technologies/videoconferencing/index.shtml

9.4 Personal Mobile Devices (PMDs) including iPads, phones and other PMDs provided by school

9.4(a) The school allows staff to bring in PMDs for their own use. Under no circumstances does the school allow a member of staff to use an identifiable PMD to contact a student using this

method. Staff are advised not to contact a parent/carer using their PMD but there may be circumstances concerning a duty of care to students which override this.

9.4(b) Students are allowed to bring PMDs to school – use of these is covered by our mobile phone policy.

9.4(c) The school is not responsible for the loss, damage or theft of any personal PMD.

9.4(d) The sending of inappropriate (as determined by any involved party) text messages between any member of the school community is not allowed.

9.4(e) Permission must be sought before any image or sound recordings are made on these devices of any member of the school community

9.4(f) Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

9.4(g) Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, these devices must be used.

9.4(h) Where members of staff use PMDs to access school services such as email or the intranet, they should not download personal information such as lists of student names to their phone.

9. 4(i) We strongly advise the use of password protection for their PMD in case of theft, and any staff losing a PMD which is configured for school data services must report the loss to the school as soon as practical. School will then prevent further access by the device.

10. Further Guidance

Websites offering help and advice:

- http://www.anti-bullyingalliance.org.uk
- http://www.itgovernance.co.uk/
- http://www.thegrid.org.uk/schoolweb/safety/webcams.shtml
- http://www.thinkuknow.co.ukc
- http://www.ceop.gov.uk/
- http://www.getsafeonline.org/
- http://www.parentscentre.gov.uk/flash/safety/main.swf
- http://www.kidsmart.org.uk/
- http://www.microsoft.com/athome/security/children/default.mspx
- http://www.parentscentre.gov.uk/
- http://schools.becta.org.uk/index.php?section=is
- http://publications.becta.org.uk/display.cfm?resID=32424&page=1835
- http://www.digizen.co.uk/
- http://www.portal.northerngrid.org/ngflportal/custom/resources_ftp/client_ftp/ e-Safety_audit_tool/e-Safety_audit_tool.html
- http://www.nextgenerationlearning.org.uk/safeguarding

11. Procedures for Handling and Reporting Incidents

11.1 Student e-safety incidents

Many incidents of misbehaviour involving ICT do not lead to actual or potential significant offence, harm or distress. These should be dealt with by our normal discipline procedures. Where the member of staff involved believes the event to be an e-safety incident, they will follow this procedure:

11.1(a) Log the incident via email to the safety coordinator. This fulfils the duty to inform the e-safety coordinator. This is a neutral log – not a punishment – however see 11.1(b) regards issues that merit further sanction.

11.1(b) If the incident constituted misbehaviour the member of staff must add a negative comment to Behave.

11.1(c) The e-safety co-ordinator investigates and decides whether further action should be taken.

11.1(d) Further action may include sanctions or education and may involve parents. In extreme cases, it may be necessary to involve outside agencies such as the Police or the local authority.

11.1(e) The e-safety co-ordinator will inform pastoral staff as appropriate.

11.2 Staff e-safety incidents

If a member of staff suspects another member of staff has breached this policy, they should report their concerns to the ESafety co-ordinator or any member of SLT. The E safety co-ordinator will investigate to see if further action is needed and report to the Headteacher. Any internal disciplinary action taken will conform to the Staff Discipline policy. If a criminal offence has been committed, the details will be passed on to the appropriate authorities.

Appendix 1

Student ICT Acceptable Use Policy (AUP) 2018/19

The school has provided ICT Equipment for use by students, offering access to a vast amount of information for use in studies, acting like an extension to the school library and offering great potential to support the curriculum.

The computers/laptops and printers are provided and maintained for the benefit of all students, and you are encouraged to use and enjoy these resources, and help to ensure they remain available to all. You are responsible for good behaviour with the resources and on the Internet just as you are in a classroom. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

The following ICT Policies must be adhered to at all times;

- **ICT Equipment Usage Policy** – Safe & effective use of ICT Resources
- **Student Printing Policy** – Limit Printing and Appropriate Use
- **Data Storage Policy** – Defines file types allowed and appropriate Use
- **Internet & E-Safety Policy** – Safeguarding Children Online
- **Security & Privacy Policy** – Accountability and Data Protection

In addition to the ICT Policies the following School Policies must also be adhered to:

- **Anti-Bullying Policy** – in particular cyber bullying
- **Health & Safety Policy**

The above policies can be found in electronic format via the students desktop or via the schools Website/VLE from September 2009 onwards. Also paper copies are available on request via Student Services or the IT Office.

The ICT Policies and Procedures are subject to change and review at any time without prior notice. It is recommended that students read through these ICT policies at least once a term.

If you have any queries or concerns then please contact **Mr M Khanna (ICT Network Manager)**

Please read this document carefully. Only once it has been signed and returned will access to the ICT Resources be permitted. If you violate these provisions, access to these Resources will be restricted and you will be subject to disciplinary action. Additional action may be taken by the school in line with existing policies regarding school behaviour. For serious violations, suspension or expulsion may be imposed. Where appropriate, police may be involved or other legal action taken.

Please complete and return this form to either Student Services or the IT Office
Year 7 New Intake – please return this form in the pre-paid envelope to the School.

I have read and understand the above and agree to use the school computer facilities within these guidelines.

Student Name:.....Signature: .....
Reg Group:.....

I have read and understand the above.

Parent/Guardian Name:..... Signature: .....

Date:.....

As the Parent, or legal guardian, of the pupil signing the above I also grant permission for my child to have Internet
Access in line with the Internet and E-Safety Policy. **Yes / No**

Image Release Form

Dear Parents,

As you may be aware, Rainhill High School often takes photographs of our students for display and publicity purposes. We have a school magazine and are keen to celebrate the success and achievements of our students in the local press. Such images may also appear on our website, in printed or electronic publications, or both.

However, before using any images of your children in publicity material we need your permission. You have our assurance that any photographs taken will be appropriate and relevant to a school activity but may we remind you that websites can be viewed throughout the world, not just in the United Kingdom where UK law applies.

If you are happy for your child to be included in school publicity materials, then no further action is required. However, if you **do not** wish your child to be involved in any photographs involving school activities, will you please complete the attached form and return it to school at the earliest opportunity. To avoid any potential misunderstanding, it would also be helpful if you could inform your child of your preference so that they can advise school staff of your wishes if any photographic opportunities arise.

Many thanks for your co-operation with this request,

If you do **not** wish your child(ren) to appear in any photographs taken by or on behalf of Rainhill High School please sign below.

Name of parent/guardian: _____

Name of child: _____ Form: _____

Parent/ Guardian signature: _____ Date: _____

Ref: New Year 7 2013/Photo Image Release Form

ICT Policies

ICT Equipment Usage– Safe & effective use of ICT Resources
Student Printing – Limit Printing and Appropriate Use
Data Storage – Defines file types allowed and appropriate Use
Internet & E-Safety – Safeguarding Children Online
Security & Privacy – Accountability and Data Protection

- This policy applies to all school computers and devices and also any mobile and tablet devices that you use in school, and also to your online behavior towards other Rainhill high School users inside and outside of school.
- Do not record sound, video, take photographs in lessons on any device unless for an activity under the direction and permission of a supervising teacher. Do not upload online, share or broadcast any such content unless given specific permission by your teacher.
- Use of mobile devices in class is under the choice, permission and direction of the teacher.

- Electronic contact & discussions with your teacher must be respectful and professional at all times and must only be part of approved school activities.
- You must ensure that your mobile device for class use has sufficient storage capacity available for downloading school apps and performing educational activities.
- Protect our identities online by not sharing passwords, not uploading personal details of you or other

Rainhill high School users. Regularly check and review your privacy settings on online sites & accounts.

- Accessing someone else's computer, phone or tablet or school/online accounts without that person's permission is illegal.

- Always ensure that your mobile device, tablet device and any online accounts that you use have passcodes switched on, and that passcodes are not revealed or shared with others.

- Do not upload or share images, video and other content that is indecent or could embarrass or harass others, or could break the law.
- Report any suspicious online sexual approaches or threatening behaviour to the E Safety Coordinator/Network Manager or teacher, and also to the authorities (CEOP) where appropriate.
- Do not publish or share any information that defames, undermines, misrepresents, or tarnishes the reputation of the school or its users.
- Do not bully others online, and report any harassment or bullying to the E Safety Co-ordinator/ Network Manager or teacher.

- Do not access unsuitable or inappropriate material online.

- Back up any important work by making a copy and storing it somewhere else that is safe.

- Copying files (images, music, video, text) that are copyright protected is against the law.

- Do not install software onto the school network, or try to circumnavigate any of the network and ICT controls that are in place.

- The school may monitor your use of IT systems and online behavior to maintain safety and also compliance with his policy.

1. Use of Mobile Learning technologies and school WIFI

Use of pupil tablet devices (iPads) to support teaching and learning activities is expected, and the content of this policy also applies to this use. Separate guidelines on classroom use of tablet devices (iPads) are issued to pupils and teachers. The school reserves the right to monitor, remove, reconfigure, and suspend use of pupil owned iPads and content to ensure compliance with this policy. The recording of sound, images or video in lessons by pupils is at the direction and permission of the supervising teacher. Do not upload online, share or broadcast any such content unless given specific permission by your teacher. Mobile devices should have passcodes set, 'find my ipad' (or similar) settings switched on, not be left out of sight and should be locked when not in use. Use of a mobile device in lessons is at the permission and direction of the supervising teacher. You must ensure that sufficient capacity is available on your mobile tablet device for school educational activities.

2. Protecting our identities online

Be aware that identity theft is an online danger that is increasing, and you should take precautions to prevent this happening. Do not upload or reveal your, your families or other Rainhill High School users' personal details online (e.g. address, phone number, date of birth, financial details, passwords, etc.) Do not upload any images and/or comments that could embarrass you or other Rainhill High School users and families – once uploaded it is often difficult or even impossible to remove such online content. Be aware that uploading digital photographs taken from a mobile device may reveal your precise GPS location at a given date and time, and therefore may reveal your movements and locations to those you would wish not to know. Avoid using your own photographs to identify yourself online, try to use an avatar or cartoon images instead.

3. Protecting yourself from Internet dangers

Report any suspicious or inappropriate sexual approaches, messages or similar online behaviour to your parent, houseparent or teacher; you may also report serious or urgent suspicions to the police by using the CEOP button available on many online chat & social networking sites, or seek help via the CEOP website. Do not store, transmit, or distribute any inappropriate or revealing images of yourself or others.

4. Use of chat, blogging and social networking facilities

These and similar facilities should be used safely, responsibly and not to excess, and should be accessed at times agreed by your supervising member of staff in accordance with school rules. You must not use offensive, derogatory, racist, sexist, unpleasant language comments/audio/imagery that could embarrass the school or its users, on any app, chat, blogging, e-mail, messaging, VLE or similar internal or external system. Please ensure that when using any such sites that your security and privacy settings are set to protect the safety and identity of you and your friends. Electronic contact with your teacher must be respectful and professional at all times, and must be only as part of approved school activities.

5. Online publication of Rainhill High School-related information

You must not submit or publish information about Rainhill High School, or any of its users, or its logo unless part of an approved educational activity. This includes using apps, micro-blogging sites such as Twitter, blogging, social networking, personal web pages, VLE, e-mail systems, text, online forums & chat or any other web- based public information and collaboration systems, and any app service.

Where information relating to Rainhill High School or its members (staff or pupils) is to be published online, the content must not defame, undermine, misrepresent, or tarnish the reputation of the school or its users.

6. Online bullying

Using apps, e-mail, text, messaging, chat, VLE, social networking, blogging, or any other electronic method to send or publish offensive or untrue messages or post unpleasant comments/imagery that could intimidate, harm, or humiliate other Rainhill High School users or their families, is forbidden and could also be breaking the law. This includes 'trolling'. (Please refer to the school anti-bullying policy and anti-cyber bullying policy).

7. Staying within the laws

What you do or say online is covered by a number of laws, and increasingly people are being prosecuted for offensive and illegal comments made by electronic communications, and on sites such as Twitter, and Facebook etc., so think before you post online or send. Unauthorized access to IT systems, accessing others' social networking accounts, e-mail accounts etc., without their permission is an offence under the Computer Misuse Act.

8. Personally owned computing & mobile devices

Regardless of the ownership of such devices (laptops, PDA's, Smart phones, tablets, digital cameras, mobile phones etc.) the school rules still apply to the use of such devices inside and outside of school where such use relates to Rainhill High School activity, and therefore the guidelines described within this document apply when such devices are being used. You must only use such devices in accordance with instructions from your teacher/houseparent, and in accordance with school rules.

9. Use of the Internet

Use of the Internet may be monitored where concerns have been raised, and a web-filtering system is in place. You must not access, store or share 'unsuitable' or illegal material on any school IT system or your own tablet or personal IT/telephony devices, or try to bypass our filtering or password security controls. Access to unsuitable content includes: gambling, pornography, promotion of bullying, proxy bypass sites, or sites inciting hatred of a particular group. Where internet access is gained outside of the school network e.g. via Mobile

3G/4G, the same rules apply in terms of not accessing 'unsuitable' material. Any access to unsuitable content, whether intentional or accidental, must be reported to the supervising member of staff and IT support.

10. Logons

By logging onto the school network, your iPad, and any other school IT systems, you agree to the guidelines and policies for ICT use at Rainhill High School. You are responsible for any activity that takes place using your school logon or any other password protected system. Your passwords for the school network and any other online facility must be kept secret and must be changed regularly. Inform IT support if you believe someone has obtained your passwords. Use passwords that are difficult to guess, and do not let anyone see you entering your passwords. It is good practice to have different passwords for different systems rather than the same password for all. Do not log on to a computing device or any ICT system using another person's password, or use such devices or systems that have been left logged on prior to your use.

When you have finished a session, exit and close any IT systems and always log off computers and any password protected sites.

11. Network Folders

School network folders, including VLE content and folders, are school property and should therefore be used for the storage of school-related work only. Student network and VLE folders may be scanned from time to time, and the school reserves the right to remove or delete any non-educational content without notice.

12. Monitoring

Rainhill High School has the right to monitor the ICT activity of students to ensure safe and proper use of its IT systems and to protect its members (staff and pupils).

13. Software

Software is not to be installed on any of the ICT facilities. Downloading or the installation of executable files (.exe) is forbidden.

14. Backing-up work

Files stored on the school network drives are regularly backed up by IT Support, however it is your responsibility to back up important work, by regularly transferring copies home, or storing electronic copies of work in a safe place. If you have lost work on school IT systems, please contact IT support to attempt recovery of files. You are responsible for the safe storage and backing up of work held on online services and websites. Always keep a copy of material stored in Cloud-based services, as these provide no guarantee of safety or security. When using mobile devices important work should be saved to the school network.

15. Copyright

You must not copy or store files, documents, music, video, or any other material where copyright restrictions exist, unless permission by the copyright holder has been given. Any external work that is used by you in your studies & in coursework should be clearly referenced and acknowledged in accordance with examination board guidelines. Using copyright material without permission is an offence under the Designs Copyrights and Patents Act.

16. Prevention of viruses

It is recommended that you have suitable anti-virus protection at home and on any personal computing/mobile devices that you use. Free Anti-Virus can be found on the schools website for staff http://www.sthelens.org.uk/sophos/
Do not open attachments to e-mails or click on links if you are suspicious or uncertain who the sender is. Do not introduce to the school network any removable device (e.g. USB memory stick) that you suspect is infected. If you suspect a virus is present on any school system, please contact IT support.

17. Protecting the school network

You must not attempt to gain administrative access to the School's network or bypass security restrictions. If you discover a problem with the School's network security, do not demonstrate the problem to other users. Instead, you should report it immediately to IT support. The Computer Misuse Act 1990 makes it a criminal offence to gain unauthorised access to a computer system in order to view or change information. The School reserves the right to inspect data files and network logs in order to investigate complaints.

18. Liability

Users' work areas are scanned daily for the presence of viruses, and files are automatically disinfected, but the School accepts no liability for any damage caused by computer viruses, however they originate. The School accepts no liability in the unlikely event that damage is sustained to your computer/tablet/mobile device as a result of its being connected to our network. Although our systems offer a very high level of protection, the School can ultimately accept no liability for data loss or its consequences.

19. Printing

You can print from networked computer locations at school, but there will be a Papercut charge to department. Please do not tamper with, maintain, or install cartridges in printing devices. Please report any faults or problems to a supervising teacher or IT support. Printing is limited on some Printers for students 10 pages at once to prevent waste and misuse. Do not treat printers as photocopiers please liaise with the schools reprographics manager for multiple copies of work for distribution.

20. Use of ICT rooms and equipment

ICT rooms and equipment must be left in good order; any damage must be immediately reported to your supervising teacher or to IT Support. After each reported incident an "IT Services Lost and Damaged Property Report" must be completed by a member of staff. Staff must use dashboard to book mobile devices and bookable rooms (Apple iPads/Laptops). Staff are accountable for looking after Devices and the rooms, when teaching their class.

Declaration

By using personal, online, and school-provided ICT facilities and systems at Rainhill High School I agree to comply with the rules described in this document and:

1. I understand that the school has the right to take action against me if I am involved in incidents of inappropriate behaviour through my use of ICT, in school and when I am out of school and where such incidents involve my membership of the school community.

2. I understand that if I fail to comply with this agreement, I may be subject to disciplinary action. This may include: loss of access to facilities, removal of personally owned tablet/mobile/web enabled devices, detentions, suspensions, and contact with parents and in the event of illegal activities, the involvement of the police.

3. I understand that this agreement covers my use of school ICT systems and equipment, and my use of my own equipment in school when allowed (e.g. laptops, tablets, mobile phones, PDA's, cameras etc.). This agreement also covers my use of my own equipment out of school and my use of online facilities when its use impacts on me being a member of the school community.

4. The specifics of this document are subject to change as technology evolves, and I understand that the intent of this document will still apply, and further guidance from time to time will be communicated to me.