E Safety Policy

Vision:	We collaborate, support and challenge each other in our endeavour to provide a world class education that allows our whole community to flourish.
Rationale:	We have a duty to provide students with adequate internet access. We understand the responsibility to educate our students on eSafety 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.

Author:	Paula Parker/Thirza Partovnia
Policy Date:	January 2019
Review date:	January 2021
Approved by:	Local Governing Body Associates
Date of approval:	Reviewed December 2018 Approval - 14th March 2019

Introductory Statement

At Rayner Stephens High School we have a duty to provide students with adequate internet access. We understand the responsibility to educate our students on eSafety 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.

Technology is seen as an essential resource to support learning and teaching, as well as playing an important role in the every-day lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to ensure our young people have the necessary skills to access life-long learning and employment. At Rayner Stephens the internet and other digital and information technologies are powerful tools and using PCs, mobile electronic devices and remote access connectivity all enable improved learning opportunities, communication and facilitate the sharing of data and resources. The technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

All network activity and Internet access in school must be in support of education and or research and must be appropriate to the educational objective of the school. It is important that all network users are aware that systems are in place to track and record what is happening across the schools ICT systems.

This policy applies to all members of the school community, including; staff, students, volunteers, parents/carers, visitors and community users, who have been granted a user account or access to the schools ICT systems both in and out of school by remote connection.

As a school we will take all reasonable precautions to ensure that users only access appropriate material. We aim to have a managed system in place, rather than a 'lock down' system, however due to the international scale and nature of the internet it is not possible to ensure that inappropriate material will never appear on a school computer. Whilst this policy will cover how risks will be managed in a school setting, further and ongoing education of students and parents/carers is required to ensure that these same risks which may feature more prominently through the use of mobile devices and PC's at home can be effectively minimised. In addition, we believe that it is essential for parents/carers to be fully involved with promoting e-Safety. Working alongside parents/carers is an important part of passing the key message to students and gaining the support for e-safety outside of the school environment.

The students and staff at Rayner Stephens High School should have an entitlement to safe internet access at all times. An integral part of managing eSafety is to ensure effectively monitor the appropriate use of the schools ICT systems. However, if misuse is an issue, steps to restrict or prevent access will be put in place to safeguard the individuals and network infrastructure.

Policy Details

This policy is written in accordance with Aspire Plus Educational Trust guidelines and has been checked against the keeping children safe in education strategy guidance, September 2016. It builds on the Tameside e-Safety policy guidance and with reference to the Inspecting E-Safety, Ofsted, 2014 focuses on each individual technology currently available within Rayner Stephens High School. It outlines the procedures in place to protect users and the sanctions to be imposed if these are not adhered to. This policy ensures that users of electronic media at Rayner Stephens are made aware of the issues and concerns and receive ongoing education in choosing and adopting safe practices and behaviours.

The school's e-safety policy will operate in conjunction with other Rayner Stephens policies including those for Behaviour Policy, Staff code of conduct. Anti-bullying, Curriculum, Safeguarding, Data Protection, Complaints and Security.

The Designated Safeguarding Officer for the school is Mrs Paula Parker (Inclusion Leader), her Deputy is Mrs Charlotte Gaskell (Family Liaison Officer). The e-Safety Coordinators for the school are Mrs Paula Parker and Mr Simon Bond (Network Manager).

The Policy was approved by the school Governors and ratified at the Local Governing Body Associates Meeting.

Roles and Responsibilities

The Headteacher is ultimately responsible for ensuring the safety of students and staff at Rayner Stephens High School. The Headteacher, Safeguarding Officer and the e-Safety co-ordinators are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff or student. Please refer to safeguarding policy.

All suspected misuse must be reported to the e-safety co-ordinators or the Headteacher in the form of written communication. Please refer to behaviour policy.

Rayner Stephens school staff are aware that we all have a duty of care and should do our best to monitor the learners ICT activity when we provide electronic devices or computer access in our learning and teaching activities.

Ensuring e-Safety

1. Ensuring a Secure Network

Rayner Stephens High School Internet access is designed for whole school use and includes filtering appropriate to the user group (Staff, Administration and Students). We will aim to ensure that filtering systems are fully functional and live to protect students and staff and we will regularly review the systems we have in place and improve them when necessary.

As a school, we will take all reasonable precautions to ensure that users only access appropriate material.

Users must access the network using their own account and passwords. These must not be disclosed or shared. Users must respect confidentiality and attempts should not be made to access another individual's personal folder on the network without permission.
The subject of e-safety will be covered as part of the curriculum throughout each academic year with reminders of this protocol to all classes.

Staff passwords will be changed every 6 weeks. The network manager has responsibility to ensure this is taking place.

Supply teachers are given log-on details and passwords as part of the booking in process.

All files downloaded within the school from the internet or received via email are automatically checked for any viruses using the schools anti-virus systems.

Software should not be installed without prior permission from the Network Manager. Removable media (e.g. pen drives / memory sticks, CD-ROMs) must be scanned for viruses before being used on a machine connected to the network.

If any machine, e.g. laptops are not routinely connect to the school network, it is the staff's responsibility to make provision for regular virus updates to take place.

All staff should be mindful that Internal emails are encrypted by default and are encrypted between the schools, and are safe for exchanging sensitive information, external e-mails should not be used to transfer staff or student personal data. Secure, approved systems such as school to school transfer or collect should be used.

If staff suspect there may be a virus on any school ICT equipment, they should stop using the equipment and inform the network manager immediately.

Machines must never be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked.' (Ctrl+alt+del followed by 'enter'). This is the responsibility of the user. Machines must be 'logged off' correctly after use.

Staff should use their professional judgement as to which place they are working in when dealing with confidential material, e.g. assessment student data.

Students must not use the teacher's machine in any of the classrooms, unless they have been given permission to do so and are logged on as themselves.

Access to the school portal by both students and staff from a remote location allows the user to effectively access their school 'desktop' and all files on the network. It is therefore important that staff and students adhere to the same security measures as is expected of them when accessing documents and information from within school. For example, locking computers when not in use, ensuring nobody has indirect access and logging off all programmes.

Access by staff to the school wireless network can only be granted by the Network Manager. This is a secure network which can be accessed through staff's individual log in details. The network is encrypted to prevent outsiders from being able to access it.

2. Procedures for Use of the Internet and Email

All users must sign an Acceptable Use Policy (appendix A and B) before access to the Internet and email is permitted in the school. This is the responsibility of the Network Manager to ensure this is completed as appropriate. This will generally be at the start of each academic year, if there have been any changes. However, if there have been no changes the document will just be to Year 7 students and in year admissions. For staff, it will be new starters or again, if there have been any changes to the document. This is further enforced through the system asking all users to make an informed choice to accept the AUP every time they log onto the system.

As a school we aim to manage all accounts effectively and ensure we have up to date account details of all users. We do not publish personal e-mail addresses of students or staff on the school website.

Currently we do allow students to send or receive e-mail from external providers.

The Internet and email should only be used for professional or educational purposes and Students must be supervised at all times when using the Internet and email.

Procedures for Safe Internet use and sanctions applicable if rules are broken will be clearly displayed in each computer suite with access to the Internet.

Both the Internet and email at Rayner Stephens use filtering software to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of 'spam,' junk or unwanted correspondence. This is to be reviewed and updated regularly. This is the responsibility of the Network Manager. All staff are responsible for reporting any inappropriate websites or content.

Internet and email use will be monitored regularly in accordance with the Data Protection Act. This is the responsibility of the Network Manager who will be overseen by a member of the Senior Team. Staff are kept well informed of the expectations through signing the Acceptable User Agreement.

Users must not disclose any information of a personal nature in a school email or on the school Internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified.

All emails sent should be professional, courteous and the formality and tone of the language used appropriate to the reader. The Network Manager will set up filtering options on the school e-mail which ensures that all e-mails which contain any inappropriate language will bounce back to the Network Manager and e-Safety Co-ordinator.

Bullying, harassment or abuse of any kind via email will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this acceptable user agreement. If users are bullied, or offensive emails are received, this must be reported immediately. Please refer to anti-bullying policy. Emails received should not be deleted, but kept for investigation purposes.

3. Curriculum and Safety

E-Safety should be acknowledged in all areas of the curriculum and staff will reinforce e-safety messages in the use of ICT across the curriculum. In developing school e-safety, skills will be embedded and activities extended and developed through both discrete ICT and cross curricular application.

In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that staff are able to quickly deal with any unsuitable material that is found on the internet searches.

Although we have safe search enabled as standard, where students are allowed to freely search the internet, e.g. using search engines, staff will still need to be vigilant in monitoring the content of the websites visited and frequently review to ensure the students are on track and focussed.

Throughout all year groups all staff, through their teaching, should encourage students to be critically aware of the materials and content they access on-line and should be guided to validate the accuracy of the information to find.

All users should be made aware of Copyright law through curriculum lessons and will acknowledge the source of any text, information or images copied from the Internet.

4. Procedures for Use of Instant Messaging, Chat Rooms and Social Networking Sites.

The use of instant messaging (e.g. MSN messenger) is not permitted at Rayner Stephens. Staff and students are not given access to instant messaging downloads, websites or applets.

Through using the school network the use of social-networking websites (e.g. Snapchat, MySpace, Facebook, Instagram, Piczo, etc.) is not permitted. Staff and students are not given access to social networking sites. The Network Manager can grant staff access to social networking sites if the access is needed to solve an issue of cyber bullying which has origins outside of school.

It is acknowledged that the use of the social-networking websites is inevitably on the increase outside of the school environment and both staff and students are made aware of the guidance that is in place, 'Using Social Media Responsibly, December 2011' as provided by the Local Authority. This document is saved on the shared drive for all staff to access and the key messages are reinforced to students via the curriculum as mentioned above. Students will also be made aware of these key principles as part of the curriculum.

Through using the school network, students and staff must not access public or unregulated chat rooms. All chat rooms websites are filtered where possible and unavailable to all Rayner Stephens users. This is regulated in school directly and monitored and updated by our Network Manager.

YouTube is a useful teaching resource and is available for use by staff, however it is not currently available for use by students as the norm. Inappropriate videos found by students or staff should be reported to the Network Manager who will take the appropriate action. Similarly, Google Images are used as a resource, whilst Safe Search is set as a default and is not editable for students some images may deemed inappropriate. In these cases the Network Manager will deal with appropriately.

5. Procedures for using digital and video images of Children

Permission must be obtained from a child's parent or carer before photographs or video footage can be taken. This is the responsibility of the Safe Guarding Lead, with support from the Family Liaison Officer. Images of Looked after Students and students for whom consent has not been given should not be photographed or videoed for any reason.

All photographs or video footage of students taken will be downloaded immediately and saved into a designated folder. This will be accessible only by authorised members of staff. Photos and videos taken on digital media will be deleted immediately once no longer needed.

For trips, staff should always prearrange to use school cameras. The staff member should not use their own camera or video recorder or phone during a trip to take or save images and/or video footage.
Students should not accept files sent via Bluetooth to their mobile phones by an unknown individual. If they do, and the content received is upsetting or makes them feel uncomfortable, they should report this. Refer to Safeguarding and Anti-Bullying Policies.

Video conferencing equipment and webcams must be switched off (disconnected) when not in use and the camera turned to face the wall where possible. Video-conferencing is the only time when webcams are used with Students and should only be used with an adult present.

Staff Student Electronic Communication
Staff should only use their e-mails for professional purposes and never share their personal e-mail with a student on roll at Rayner Stephens. The only acceptable method for a student to communicate electronically with a member of staff or another student is via the school e-mail or VLE.

If staff are communicating with students via the VLE, in terms of setting homework or uploading resources for example, this must be used appropriately and professionally in line with teacher standards and the school's code of conduct.

All Rayner Stephens staff are strictly prohibited from accepting or inviting Rayner Stephens students as "friends" on social networking sites such as Facebook. For social networking expectations please refer to point 4 of this policy.

Friendships requests made by ex-students may only be accepted by staff when:

- The student has left Rayner Stephens and turned the age of 18
- The student has no known siblings currently educated at Rayner Stephens
- Any exceptions to this may be given to the Headteacher for consideration

Staff have a responsibility to report any incidents where they have either been requested to make contact or have been in electronic contact with students outside of school hours. These incidents should be reported to the Safeguarding Officers in the first instance.

Students will be educated through assemblies, form tutor curriculum, PSHE, and through the wider curriculum that adding or requesting staff as friends on social networking sites is against school e-safety policy and that there is a professional expectation of both parties that the teacher-student relationship be maintained both inside and outside of the classroom.

All staff are responsible for ensuring the content of any social networking page they possess could not in any way be seen to be bringing the school into disrepute or making themselves vulnerable to having their professionalism questioned.

There will be no formal monitoring of staff or student use of social networking sites outside of school hours as it is the responsibility of the individual to ensure their online actions maintain the high expectations of professionalism the school sets for both staff and students.

6. Staff Parent/Carers Electronic Communication
Staff may choose to communicate certain messages through the use of the schools Communication System. The ParentMail system will allow for short texts to be sent covering key

messages. To ensure the number of texts and the tone of the message is appropriate this is overseen by the Deputy Headteacher who has responsibility for Safeguarding.

7. Procedures to ensure safety of the Rayner Stephens website

Rayner Stephens has a designated member of staff who is responsible for approving all content and images to be uploaded onto its website prior to it being published. For the academic year, this is the Operations Manager with support from the Director of Finance and Resources.

It is the responsibility of the Director of Finance and Resources along with the Operations Manager to carry out checks to ensure that no material has been inadvertently posted, which might put students, staff or the school at risk. Copyright and intellectual property rights must be respected.

Permission is obtained from parents or carers before any images of students can be uploaded onto the Rayner Stephens website. Names are not used to identify individuals portrayed in images uploaded onto the Rayner Stephens website. Similarly, if a child / young person or member of staff is mentioned on the website, photographs which might enable this individual to be identified do not appear.

When photographs to be used on the website are saved, names of individuals should not be used as file names.

8. Procedures for using mobile phones or other mobile devices

It is understood staff, at their own risk, will have personal mobile phones with them in the school day and it is expected that these will only be used at appropriate times throughout the day. Personal phones are not to be used to make contact with parents and if essential, steps must be taken to disclose the personal phone number. Work mobile phones that are provided by the school must always be available for use in the event of an emergency and must only be used for school business. Students are required to switch mobile phones off during the school day. However, they may be used at break and lunch time as a privilege. Any personal mobile phones which are brought into school are done so at the individuals own risk.

The taking of still pictures or video footage on staff's personal phones is not permitted. The use of phones, equipment provided by school must be used and pictures/footage only taken/used with parents' permission. School declares the right to view the content of any mobile phone which may have been used in this way in order to protect the individual. Video footage of a serious incident such as fighting found on individual's phone will be punishable by confiscation of the phone and parents being contacted. Similarly, for instances where staff feel there has been a continued invasion of privacy through a students use of a camera phone or inappropriate digital images or videos have been downloaded and viewed during school hours. Refer to the behaviour policy.

It is the responsibility of the Safeguarding Lead to ensure the curriculum and assemblies spend enough time making students aware of the safe practices involving mobile phones. Including educated students on who the key people in school are if they are the recipient of hurtful or unwanted calls or text messages. The Safeguarding Officers must be informed of any case of cyber-bullying. The school also has a responsibility to educate students in what to do if they are contacted by someone who is unknown to them.

9. Sanctions to be imposed if procedures are not followed

If procedures in the policy are not followed by students then the following sanctions may be used by school staff in line with school behaviour policy:

- Contact with parents or carers
- Detention
- Users may be suspended from using the Rayner Stephens computers, Internet or email for a given period of time / indefinitely
- Items may be confiscated
- Content of electronic devices may be checked by a member of staff
- Details may be passed on to the police in more serious cases or as deemed appropriate by the Headteacher.
- Legal action may be taken in extreme circumstances or as deemed appropriate by the Headteacher.

If these policy procedures are not followed by staff then it will fall to the discretion of the Headteacher to fully investigate any incidents and decide which and whether any further action will be taken.

10. Closing Statement

Rayner Stephens High School are aware that the procedures in this policy will be subject to ongoing review and modification in order to keep up with advances in technology coming into the school and that this policy will not remain static and will be reviewed once every two years. It may be that staff and students might wish to use an emerging technology for which there are currently no procedures in place. It is therefore advisable to state that the use of any emerging technologies will be permitted upon completion and approval of a risk assessment, which will be used to inform future policy updates.

Appendix A

Acceptable Use Policy (AUP): Student agreement form

Covers use of digital technologies in school: i.e. **email, Internet, intranet and network resources,** learning platform, software, **equipment and systems.**
These rules will are in place to ensure that all students are aware of their responsibility to make safe and informed choices, both in and out of school.

1. I will only use the school's computers for schoolwork, homework and as directed.
2. I will not bring files into school (on removable media or online) without permission or upload inappropriate material to my workspace.
3. I will only edit or delete my own files and not view, or change, other people's files without their permission.
4. I will keep my logins, IDs and passwords secret.
5. I will use the Internet responsibly and will not visit web sites I know to be banned by the school. I am also aware that during lessons I should visit web sites that are appropriate for my studies.
6. I will only e-mail people I know, or those approved by my teachers.
7. The messages I send, or information I upload, will always be polite and sensible.
8. I will not open attachments, or download a file, unless I have permission or I know and trust the person that has sent them.
9. I will not give my home address, phone number, send photographs or video, or give any other personal information that could be used to identify me, my family or my friends.
10. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room. If someone makes an invitation of this type: I will alert an adult in school or at home.
11. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will save it and talk to a member of staff.
12. I am aware that some websites have age restrictions and I will comply with this.
13. My online activity will not upset or hurt other people and I will not put myself or others at risk.
14. I will respect and not damage any equipment in school. If an accident occurs I will inform a member of staff immediately.
15. I will not log onto any computers using any other person username and password. If I find a computer that has been left logged in I will only use it log the person out.

Acceptable Use Policy (AUP): Student agreement form

User Signature

I agree to comply with all the points above.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature .... Date ....

Full Name .... (printed)

Appendix B

Acceptable Use Policy (AUP): Staff agreement form

Covers use of digital technologies in school: i.e. **email, Internet, intranet and network resources,** learning platform, software, **equipment and systems.**

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / Aspire Plus Educational Trust systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols, documented in the Safe Working Practice Policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business. (This is currently Office 365. (portal.office.com))
- I will only use the approved school email, school Learning Platform or other school approved communication systems with students or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues or others.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of students or staff without permission and will not store images at home without permission.
- I will use the school's Learning Platform in accordance with school protocols.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I am aware of the Using Social Media Responsibly guidance, within the Safe Working Practice policy in the that is available from the Aspire Plus Educational Trust and I will adhere to this alongside any other information as provided to me by the school
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.

- I will access school resources remotely (such as from home) only through the School Portal / school approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or student information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching.
- I will alert the school's named safeguarding officers/ relevant senior member of staff if I feel the behaviour of any child I teach may be a cause for concern.
- I will only use the school systems in accordance with any corporate policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or students), which I believe may be inappropriate or concerning in any way, to a senior member of staff / named child protection officers at the school.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

I agree to comply with all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature .... Date ....

Full Name .... (printed)

Job title ………………………………………………….. School ………………………………………………

Authorised Signature

I approve this user to be set-up.

Signature .... Date...

Full Name .... (printed)