Regency High School
E-Safety Policy

Written by: Sara Harding
Authorised by: Chair of Governors

Date: September 2017
Review Date: September 2019

Signed by: ..... (Policy Author)

Date: .....

Signed by: ..... (Chair or Governors)

Date: 14/03/2018.

Contents

E-safety Policy Details

E-safety Lead: Mrs Kate Jasper

Designated Safeguarding Lead: Mr. Michael Eglesfield

Designated Deputy Safeguarding Lead: Mrs Sara Harding

Ratified by Governing Body on:

Next review date: September 2019

1. Introduction

1.1. Regency High School embraces the positive impact and educational benefits that can be achieved through the appropriate use of the Internet and associated communications technologies.

1.2. However, we are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, Regency High School aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

1.3. The policy has been developed in consultation with the Senior Leadership Team and Governing Body

2. Scope

2.1. This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the school and to personal devices owned by adults or pupils and used whilst on the school premises.

2.2. Where possible, this policy has been explained to the pupils of the school so that:

- They understand that there are dangers associated with the Internet and associated mobile technologies
- They know what behaviour is expected of them
- They know what to do if they encounter unacceptable, undesirable or inappropriate use

2.3. Definitions of unacceptable, undesirable or inappropriate use within this policy may relate to any of the following:

2.3.1. Undesirable materials

- Pornographic images or obscene text
- Language that is abusive, profane, inflammatory, coercive, defamatory, blasphemous or otherwise offensive
- Racist, exploitative or illegal materials or messages

2.3.2. Undesirable contacts

- E-mail or instant messages from unknown or unverified parties, who seek to establish a child's identity and/or to communicate with them, such as for advertising or potentially criminal purposes

2.3.3. Unacceptable use

- Deliberate searching for, and accessing of, undesirable materials
- Creating and transmitting messages that contain unacceptable language or content

- Creating and publishing materials that contain unacceptable language or content
- Cyber Bullying, abusive or threatening language
  We recognise that bullying can take place via the Internet and through the use of mobile phones. Bullying in any form is taken very seriously and is dealt with in line with school policy on bullying.
- Racial or Sexual Harassment
- Inappropriate web site access
- Gambling, unethical or illegal practices

3. Illegal or Inappropriate Activities

3.1. Regency High School School believes that the activities listed below are inappropriate in a school context and that users should not engage in these activities when using school equipment or systems in or out of school.

3.2. Users shall not visit internet sites, make, post download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images (illegal – The Protection of Children Act 1978)
- Grooming incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)
- Possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)
- Criminally racist material in UK – to stir up religious hatred or hatred on the grounds of sexual orientation (illegal – Public Order Act 1986)
- Pornography
- Promotion of any kind of discrimination
- Promotion of racial or religious hatred
- Threatening behaviour, including promotion of physical violence or mental harm,
- Any other information which may be offensive, breaches the integrity of the ethos of the school or brings the school into disrepute

3.3. Additionally the following activities are also considered unacceptable on any ICT devices provided by the school:

- Using school systems to run a private business
- Use systems, applications, website or other mechanisms that bypass the filtering or other safeguards employed by the school and Worcestershire County Council.
- Uploading, downloading or transmitting commercial software or any other copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or propriety information (e.g. financial/personal information, databases, computer/network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet
- On-line gambling and non-educational gaming

4. Roles and Responsibilities

4.1. The Governing Body

- is responsible for the approval of this policy and for reviewing its effectiveness by receiving regular information about e-safety incidents and monitoring reports.

4.2. The Head Teacher

- has ultimate responsibility for establishing safe practice and managing e-safety issues at Regency High School. She, in turn, delegates responsibility for the day to day management of e-safety issues to the Network manager and e-safety lead.
- will be familiar with the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

4.3. The E-safety Lead

- enables all staff to take day to day responsibility for e-safety issues by providing systems and information that enable them to contribute to the monitoring of ICT use in the school.
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- has a leading role in establishing and reviewing the school e-safety policy
- provides advice and access to training for staff
- liaises with the Local Authority as necessary
- liaises with the school ICT and Computing Team
- liaises with the Network manger frequently to discuss current issues and discuss incident logs
- meets regularly with the Head Teacher to discuss current issues and review incident logs
- attends relevant meetings of the Governing Body when requested to do so.
- receives appropriate training and support to fulfill their role effectively

4.4. School Staff

All school staff have certain core responsibilities within and outside the school environment. They should

- safeguard the welfare of children and refer any safeguarding concerns to the Designated Safeguarding Lead
- have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- use technology responsibly
- read, understand and sign the school's Acceptable Use Agreement for staff
- accept responsibility for their use of technology
- report any suspected misuse, incidents or problems to the e-safety lead or member of the Senior Leadership Team
- model best practice when using technology
- embed e-safety issues in the curriculum and other school activities
- understand that all network activity and online communications are monitored, be aware that in certain circumstances, where unacceptable use is suspected, enhanced monitoring and procedures may come into action

4.5. Network Manager and ICT technician ensure

- the school's ICT infrastructure and data are secure and not open to misuse or malicious attack
- the school meets the e-safety technical requirements as described in the Capita IBS School's System and Data Security advice document
- users may only access the school's networks through password protection
- any shortcomings in the infrastructure are reported to the e-safety lead or Head Teacher so that appropriate action may be taken.

5. Acceptable Use Policy Agreements

5.1. All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to school systems. In addition, any pupil or member of staff who use their own personal devices i.e memory sticks in order to access the school network or internet are also required to sign an acceptable use policy agreement.

5.2. Acceptable use policy agreements are provided for:

- Pupils (where it is appropriate)
- Staff and volunteers
- Visitor users of the school's ICT system

5.3. Pupils with severe or profound and multiple learning difficulties, who are unable to independently access the internet or mobile technologies are not required to sign an acceptable use policy agreement. Wherever possible, the acceptable use policy will be explained to pupils at a developmentally appropriate level

5.4. All users are also required to agree to an acceptable use policy before being allowed to log on to the school network. Adults working with pupils who have severe or profound and multiple learning difficulties, agree to the acceptable use policy on their behalf

5.5. All employees of the school and volunteers sign a written acceptable use policy when they take up their role in school and in the future if significant changes are made to the policy.

5.6. "Visitor users" sign when they first request access to the school's ICT system.

6. Internet Access

6.1. Central filtering of websites is provided and managed by Capita IBS Schools. Staff requiring access to a restricted site are required to submit a request to the Network Manager via the POD who will contact Capita IBS and this will be granted or denied once the website has been reviewed

6.2. Requests for changes to the filtering are directed to the Network Manager in the first instance who forwards these on to Capita IBS Schools or liaises with the Head as appropriate.

6.3. All staff and students (where appropriate) understand that if an inappropriate site is discovered it must be reported to the e-safety lead and the Network Manager who will block it with "Squid proxy".

6.4. If any incidents occur, where it is suspected that an inappropriate website has been accessed, then this will be recorded in the e-safety log book for audit purposes.

7. Email

7.1. Access to email is provided for all users in school through the Worcestershire Schools and Academies Wide Area Network and managed by the Network Manager. All staff and pupils (where appropriate) are provided with Global Ids and passwords which are used to access both email and the Worcestershire Edulink service.
To avoid pupils revealing their identification within e-mail messages:

- Only the pupil's forename is revealed

- The pupil's full name is never revealed
- The pupil's address is never revealed
- Information is never given that might reveal a pupil's identity
- Information is never given that might reveal a pupil's whereabouts

7.2. All staff are given a school e-mail address and understand that this must be used for all professional communications. Where appropriate, pupils are also given a school e-mail address that can be used for educational purposes.

7.3. Everyone in the school community who is able to use email is informed, through the acceptable use policy (and explained to pupils where appropriate), that the e-mail system may be monitored and should not be considered private communication.

7.4. The school encourages the use of e-mail to contact the school via the school office or staff e-mail addresses. The school does not publish any contact details for the pupils.

7.5. Staff are allowed to access personal e-mail accounts on the school system outside of directed time and understand that any messages sent using the school equipment should be in line with the acceptable use policy.

7.6. Pupils may be given the opportunity to check their own e-mail outside of directed time and understand that any messages sent using the school equipment should be in line with the Acceptable Use policy. In addition, they are made aware that these messages will be scanned by the profanity filter in school.

7.7. Users must immediately report, to the e-safety lead or designated safeguarding lead, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. They must not respond to such emails.

7.8. Where appropriate, pupils are made aware of the dangers and good practices associated with the use of email through the e-safety program that forms a part of the long term plan for ICT and Computing.

7.9. It is recognised that e-mail or instant messages received or transmitted by children can contain language or content that is unacceptable. It is also recognised that some people may try to use e-mail to identify and contact children for unacceptable reasons.

7.10. To help to avoid these problems the School has adopted the following practice:

- Pupil (and staff) email accounts are scanned for viruses
- The profanity email filter, filters all messages sent or received whilst the user is logged onto the school network and captures all inappropriate content that can then be reviewed by the network manager.

7.11. However, it must be acknowledged that the authority's email system is web based and can be accessed by pupils at home, as can instant messaging systems and social networking sites. Parents need to be encouraged to be vigilant also.

7.12. To avoid children revealing their identification within e-mail messages pupils are taught:

- never to reveal their address
- never to give information that might reveal his / her whereabouts
- never to reveal any other personal information that may allow strangers to identify them.

7.13. If staff believe that children have been targeted with e-mail messages by parties with

criminal intent, the messages will be retained, the incident recorded, and the Governors and the child's parents informed. Advice from the Local Authority will also be taken regarding any further action.

8. Regency High School Website

8.1. The Regency High School website can be found at http://www.regency.worcs.sch.uk/

8.2. Regency High School uses its website in order to share information with and beyond the school. This includes, from time-to-time, celebrating the work and achievements of pupils.

8.3. Personal information will not be posted on the school website and only official email addresses will be used to identify members of staff.

8.4. Pupils are not identified by name on the school website. If, for any reason, a pupils name does need to be included, only his/her first name will be used and only then following parental consent.

8.5. Pupil's work is only published on the school website following permission from their parents or carers.

8.6. The Head Teacher takes overall responsibility for content published to the school web site but delegates general editorial responsibility to the business manager.

8.7. Class teachers and subject leaders are responsible for the editorial control of any work published by their students.

8.8. The school will hold the copyright for any material published on the school web site or will obtain permission from the copyright holder prior to publishing with appropriate attribution.

9. Regency High School Twitter Account

9.1. Regency's Twitter account can be found at https://twitter.com/regencyhigh

9.2. Regency's Twitter account is currently accessed only by the Head teacher and the Network manager.

9.3. Pupils are not able to contribute to the Twitter account.

9.4. The Head teacher and the Network manager will check/moderate any content placed onto Twitter. Any concerns will be passed directly to the e-safety lead and, if necessary, the designated safeguarding lead.

9.5. The head teacher takes overall responsibility for content published to the school Twitter account but delegates' general editorial responsibility to the Network manager.

9.6. Class teachers and subject leaders are responsible for the editorial control of any work published by their students.

9.7. The school will hold the copyright for any material published on the Twitter account or will obtain permission from the copyright holder prior to publishing with appropriate attribution.

10. Anti Virus Software

10.1. Sophos anti-virus software is installed on all computers by the schools Network manager and ICT technician and is updated automatically. Any alerts are managed by the school's Network manager.

11. Monitoring of the Use of Computers, Software, Email and Internet Use

11.1. The network has installed IMPRO which is monitoring all computer activity and capturing screen shots of any activity that contains a trigger word from one of its many libraries.

11.2. IMPRO's reporting function can provide information that can be used both to identify any inappropriate use of computers and also to identify vulnerable young people who may be suffering from modern day life pressures including abuse, bullying, anxiety, and depression disorders

11.3. Monitoring of staff and pupil behaviour using IMPRO is carried out continuously and will highlight inappropriate use to the Network manager.

12. School Network Access

12.1. All staff are issued with their own username and password in order to access the school network.

12.2. Visitors or supply staff are issued with temporary ID's and have only restricted access to the school network.

12.3. All pupils use class logon ID's for their network access and then store their work in a named folder within this.

13. Access to Undesirable Materials by Children

13.1. Children at Regency High School who are cognitively able to perform internet searches are taught that they must never intentionally seek offensive material on the Internet. Any transgression is likely to be captured by IMPRO but staff witnessing this behaviour should notify the head teacher immediately. Any incident will be treated as a disciplinary matter and the behavior policy will be applied. The incident will be recorded on the school POD

13.2. If deliberate access to undesirable materials it repeated, flagrant or habitual, the matter will be treated as a serious disciplinary issue. Any incident will be treated as a disciplinary matter and the behavior policy will be applied. The incident will be recorded on the school POD. The child or children's parents will be informed and the Governing Body will be advised. The Network manager can block a pupil's access to computers on the school network if this is felt to be necessary.

13.3. Unintentional access of undesirable materials, for example when a web search yields unexpected results should also be picked up by IMPRO but, again, should be reported to the head teacher or e-safety lead if it is observed by a member of staff and recorded in the e-safety log.

14. Deliberate Access to Undesirable Materials by Adults

14.1. Deliberate access to undesirable materials by adults is unacceptable, and will be treated as a disciplinary issue. If abuse is found to be repeated, flagrant or habitual, the matter will be treated as a very serious disciplinary issue. The Governors will be advised and the Local Authority will be consulted.

15. Mobile Technologies

15.1. Teaching staff and some Teaching Assistants at Regency High School are provided with a laptop for educational use and their own professional development. All staff understand that the acceptable use policies apply to this equipment at all times and sign an agreement to this fact prior to taking ownership of the laptop.

15.2. To ensure the security of the school systems, personal equipment is currently not permitted to be connected to the school network, unless this has been authorised by the Head Teacher or E-safety lead and up to date virus software is installed where necessary.

15.3. Staff understand that they should use their own mobile phones sensibly and in line with school policy. Where pupils are able to use mobile phones, they are encouraged to understand that their mobile phones must be turned off during directed time and used in line with school policies at all other times.

15.4. The Educations and Inspections Act 2006 grants the Head Teacher the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Head Teacher will exercise this right at her discretion.

15.5. Images of staff and pupils are not to be taken on personal devices unless permission has been granted to do so by a member of the Senior Leadership Team. Any images must be transferred to the school network at the earliest convenience

15.6. New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the school community.

16. Digital Media

16.1. Regency High School respects the privacy of the school community and will obtain written permission from staff, parents, carers before any images, video or sound recordings are published or distributed outside of the school. In addition to this:

- Photographs will not identify any individual pupil
- Students' full names will not be published outside of the school environment

16.2. If external video conferencing occurs then written permission will be obtained from parents or carers prior to pupils taking part and supervision of video conferencing will be appropriate to the age and cognitive ability of the pupils

17. Social Networking and Online Communication

17.1. The school has reviewed the use of social networking sites and online communication and currently does not allow access to social networking sites. Even so, where appropriate, guidance is provided to the school community on how to use these sites safely and appropriately. This includes:

- not publishing personal information
- not publishing information relating to the school community
- how to set appropriate privacy settings
- how to report issues or inappropriate content

17.2. Un-moderated chat sites present an unacceptable level of risk and are blocked in school. Pupils are given age appropriate advice and guidance around the use of such sites

18. Educational Use of Technologies in School

18.1. School staff are expected to model appropriate use of school resources, including the internet, at all times.

18.2. Teachers will be responsible for their own classroom management when using ICT equipment and will remind pupils of the Acceptable use policy at regular intervals.

18.3. Staff and students will be expected to reference all third party resources that are used in their work

19. Copyright

19.1. It is recognised that much material on the Internet is copyright, unless this is specifically waived. It is the school's policy that the copyright of Internet materials will be respected.

19.2. Where materials are published on the Internet as part of the teacher's professional duties, copyright will remain with the County Council. Internet published materials will contain due copyright acknowledgements for any third-party materials contained within them.

20. E-safety Training

1. All staff will be expected to attend an annual E-safety update and sign the acceptable use policy Agreement for Staff and Volunteers. In addition:

- Educational resources are reviewed by subject leaders and disseminated through curriculum meetings / staff meetings / training sessions
- E-safety is embedded throughout the school curriculum and visited by each class where this is appropriate
- Where appropriate, pupils are taught how to validate the accuracy of information found on the internet
- E-safety advice is provided to parents via the school website

21. E-safety Education

21.1. Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. Wherever appropriate, the education of pupils in e-safety is an essential part of the school's e-safety provision. Pupils need the help and support of the school to recognise and avoid e-safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them. They need to be taught how to behave appropriately when accessing the internet and on-line facilities and what to do if they encounter offensive, abusive or upsetting materials.

22.2. E-safety education is incorporated into the long term plan for ICT and Computing and pupils are taught the principles contained within the SMART rules in order to help to keep themselves safe:

- S – Staying SAFE by not revealing personal information
- M – The dangers of MEETING on-line friends
- A – The dangers of ACCEPTING emails from strangers, viruses in attachments etc.
- R – Pupils deciding if information is RELIABLE and understanding that people may not be truthful
- T – The need to TELL an adult if they are worried or concerned

22.3. E-safety education at Regency High School includes:

- A planned e-safety programme provided as part of ICT and Computing and PHSE curriculum as well as assemblies and pastoral activities.
- The use of online resources such as
  - South West Grid for Learning
  - Hector's World
  - Cyber Café
  - CEOP's Think U Know website
    Username: office@regency.worcs.sch.uk
    Password: Regency101
  - CBBC Stay Safe website
  - CEOP You Tube videos

22.4. Pupils will be helped to understand the need for the pupil acceptable use policy agreement and encouraged to adopt safe and responsible use of ICT both within and outside of school.

22.5. In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

22.6. Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit, encouraging them to discuss anything of which they are unsure and implementing the expected sanctions and/or support as necessary.

22.7. Pupils will be made aware of what to do should they experience anything, while on the internet, which makes them feel uncomfortable.

22. The School E-safety Self Review Tool

22.1. Regency High School is enrolled in the on-line 360 degree safe 'School E-safety Review Tool' and progression through the tool is monitored by the head teacher and governing body. This tool enables the school to review current practice over four main elements namely:

- Policy and Leadership
- Infrastructure
- Education
- Standards and Inspection

23. Publicising E-safety

23.1. Effective communication across the school community is key to achieving the school vision for safe and responsible citizens.

23.2. In order to publicise the e-safety message, Regency High School will:

- Make this policy, and related documents, available on the school website
- Introduce this policy, and related documents, to all stakeholders at appropriate times. This will be at least once a year or whenever it is updated
- Post relevant e-safety information in all areas where computers are used
- Provide e-safety information to parents via the school website

23.3. It is important to ensure that parents are helped to keep their children safe on-line when they are at home and, as such, they are informed about the information available on the school website and advised to consult this or to speak to school staff if they require any further information or advice.

24. Data Security / Data Protection

24.1. Regency High School has a duty to ensure that personal data will be recorded, processed, transferred and made available in line with the Data Protection Act 1998 and the Freedom of Information Act 2000. Regency High School also has a responsibility to ensure that computer systems (and the information stored within them, even if this data is not classed as personal) are kept safe and secure.

24.2. Several documents are available that deal with the school's responsibilities with regard to data protection and security and these should be read in conjunction with this E-safety policy. This document is:

- School Data Protection Policy, date

25. Responding to Incidents

25.1. Inappropriate use of the school resources will be dealt with in line with other school policies, for example the Behaviour, Anti-Bullying and Safeguarding Policies and these should also be consulted for further information. Specifically with regard to incidents concerning information and communication technologies:

- Any suspected illegal activity will be reported directly to the police. The Capita IBS Schools Service Desk will also be informed to ensure that the Local Authority can provide appropriate support for the school.
- Third party complaints, or from parents concerning activity that occurs outside the normal school day, will be referred directly to the head teacher and the designated safeguarding lead.
- Breaches of e-safety policy by staff will be investigated by the head teacher or the designated safeguarding lead. Appropriate action will be taken under Worcestershire County Council's disciplinary policy where a breach of professional conduct is identified.
- Pupil policy breaches relating to bullying, radicalization, drugs misuse, abuse and suicide will be reported to the designated safeguarding lead and action taken in line with school anti-bullying and safeguarding policies. There may be occasions when the police must be involved
- Other breaches of this policy by students will be treated as any other breach of conduct in line with the school behaviour policy
- Minor student offenses, such as being off-task visiting games or email websites will be handled by the teacher in situ by invoking the school behaviour policy.

25.2. The Educations and Inspections Act 2006 grants the Head Teacher the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate

26. Professional Standards for Staff Communication

26.1. In all aspects of their work in our school, teachers abide by the Teachers' Standards. Teachers translate these standards appropriately for all matters relating to e-safety.

26.2. Any digital communication between staff and pupils or parents / carers

- must be professional in tone and content.
- must only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking technology must not be used for such communications.

26.3. Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These

evaluations help inform policy and develop practice as do any views and experiences of the pupils.

27. Acknowledgements

27.1. Material in this document is adapted from E-safety advice authored by

- Worcestershire County Council
- Birmingham City Council
- WMnet
- Becta
- The South West Grid for Learning
- Chadsgrove School E-Safety and Acceptable Use Policy

27.2. Original copyright is held by their relevant authors and their use is gratefully acknowledged.

APPENDICES

1. Acceptable use policy Agreement –Pupils Working with Severe learning difficulties
2. Acceptable use policy Agreement – Pupils with moderate learning difficulties
3. Acceptable use policy Agreement for Staff
4. Acceptable use policy Agreement for Visitor & Volunteers

Acceptable use policy Agreement –Pupils Working with Severe learning difficulties

This is how we stay safe when we use computers:

- I will ask an adult if I want to use the computer
- I will only use activities if an adult says it is OK.
- I will take care of the computer and other equipment
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will turn off the monitor and tell an adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

I understand these computer rules and will do my best to keep them

My name:	
Signed (child):	
OR Parent's signature:	
Date:	

Acceptable use policy Agreement – Pupils with moderate learning difficulties

I understand that while I am a member of Regency High School I must use technology in a responsible way.

For my own personal safety:

- I understand that my use of technology (especially when I use the internet) will be supervised and monitored.
- I will keep my personal login safe and will not use anyone else's (even with their permission)
- I will keep my own personal information safe as well as that of others.
- I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.

For the safety of others:

- I will not interfere with the way that others use their technology.
- I will be polite and responsible when I communicate with others,
- I will not take or share images of anyone without their permission.

For the safety of the school:

- I will not try to access anything illegal.
- I will not download anything that I do not have the right to use.
- I will not deliberately bypass any systems designed to keep the school safe.
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes of any type on the devices belonging to the school without permission.

I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow these guidelines:

Name:	
Signed:	
Date:	

Acceptable use policy Agreement – Staff

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, learning platform) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school in the e-safety policy.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident of which I become aware, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital images. I will not use my personal equipment to record these images.
- I will ensure that all videos/sound clips are watched in full before being used in lesson time and use the full screen view function so that advert boxes and comments are not seen
- Where images are published (e.g. on the school website) I will ensure that it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not mention the school or anything associated with it by name on social networking sites
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will not accept friend requests from children on social networking sites
- I will ensure that my personal social networking page is private

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will only use my personal mobile ICT devices as agreed in the e-safety policy and then with the same care as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up in school, which I understand will only take place automatically if files are stored on the school network.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carryout their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any intentional damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I will not take or access pupil data, or other sensitive school data, off-site without specific approval. If approved to do so, I will take every precaution to ensure the security of the data.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not allow pupils to use staff laptops / desktop PC's
- I will make sure that my portable devices will have a security pin (Network manager can help to install this)

When using the internet in my professional capacity or for sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and to my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could involve a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police
- I understand that the school might publish images, video or sound recordings outside of the school. However the photograph will not identify any individuals nor will the school publish any full names outside of the school environment.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines.

Staff / volunteer Name:	
Signed:	
Date:	

Acceptable use policy Agreement – Visitor User

You have asked to make use of our school's ICT facilities. Before we can give you a log-in to our system we need you to formally agree to use the equipment and infrastructure responsibly.

For my professional and/or personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, of which I become aware, to a member of the school's staff.
- I will not use my personal device in school to take pictures unless permissioned by the e-safety lead.

I will be responsible in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files or data, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials described above.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carryout their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, except with the specific approval of the school.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

I have read and understand the above and agree to use the school ICT systems within these guidelines. I understand that failure to comply with this agreement will result in my access to the school's ICT systems being withdrawn, that further actions will be taken in the event illegal activity, and that I may be held liable for any damage, loss or cost to the school as a direct result of my actions.

Community user Name:	
Signed:	
Date:	