Egerton Rothesay School
E-Safety and Data Security: Policy for ICT Acceptable Use

Introduction

ERS recognises that ICT and the internet are essential tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and safely.

Information and communication technology cover a wide range of resources including:

- Websites
- Learning platforms and virtual learning environments
- E-mail and Instant Messaging
- Chat rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music downloading
- Gaming
- Mobile/smart phones with text, video and or web functionality
- Other mobile devices with web functionality
- Artificial Intelligence

This e-safety policy has taken into consideration the four categories of risk known as the 4C's, which are: Content, Contact, Conduct and Commerce as outlined in our Safeguarding policy.

This e-safety policy is designed to help to ensure safe and appropriate use. The use of technology can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement, particularly with the growth of AI
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

All persons working with children and/or with responsibility for educating members of the school community have a duty of care, which includes responsibility for online safety. It is important that there is a balance between controlling access to technology and the internet and allowing freedom to explore and use these tools to their full potential. Online safety is a whole-school issue and responsibility.

The Purpose & Scope of this policy

This policy aims to:

- ensure that ICT activity in the school is well regulated and monitored
- ensure that pupils are educated about e-safety issues and appropriate behaviours so that they remain safe and behave appropriately and legally online
- provide a good understanding of appropriate ICT use that everyone in the school community can also use as a reference for their online conduct outside of school

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

Links to other relevant school policies

This policy should be read in conjunction with the following policies:

- Safeguarding and Child Protection Policy
- Anti-bullying Policy
- Behaviour Policy
- Staff code of Conduct
- Data Protection/GDPR Policy

Roles & Responsibilities

Egerton Rothesay School's online safety team consists of:

- Headteacher – Mr A Cairns
- Safeguarding Team – Ms S Vest and Ms I Holt
- IT and Network Coordinator – Mr S Potts
- Head of ICT – Mrs K Stansbury

The designated member of the Board of Directors responsible for online safety is Mr J Reynolds.

The Parents Pages and ERS website content is managed by: Mr S Potts

Online Safety Team

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, although day to day responsibility for online safety will be delegated to the Online Safety Team. Any complaint about staff misuse should be referred to the Headteacher. The Headteacher and Online Safety Team are responsible for:

- Ensuring access to induction and training in online safety practices for all users
- Ensuring all staff receive regular and up-to-date training.
- Ensuring appropriate action is taken in all cases of misuse.
- Ensuring that internet filtering methods are appropriate, effective and reasonable

- Ensuring that staff or external providers who operate monitoring procedures be supervised or overseen by the IT/ICT Co-Ordinator.
- Ensuring that any pupil or staff personal data as recorded within the school management system sent securely via the internet.
- Working in partnership with DfE guidance, the school's internet service provider and ICT/Network coordinator and Head of ICT to ensure systems to protect students are appropriate, managed correctly and reviewed and improved.
- Ensuring the school ICT system is reviewed regularly regarding security and that virus protection is installed and updated regularly and as threats are known.
- Reviewing monitoring reports, reported online safety incidents and log of incidents to inform online safety developments.
- Leading online safety meetings
- Liaising with the nominated member of the Board of Directors to provide an annual report on online safety.
- Liaising with the safeguarding team to make parents aware of potential on-line 'dangers' and to encourage close monitoring of their children's internet use.

The Headteacher and Online Safety Team, together with the external IT monitoring company and internet service provider will ensure:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements as well as any DfE, safeguarding or other online safety policies and guidance that are relevant to school.
- That users may only access the networks and devices through a properly enforced password protection policy implemented by the ICT/Network coordinator.
- The filtering policy is applied and updated on a regular basis and its implementation is the responsibility of the Online Safety Team.
- The ICT and Network Coordinator, IT Technician and Head of ICT will keep up to date with online safety technical information to effectively carry out the online safety role and to inform and update others as relevant.
- That the use of the network/internet/virtual learning environment/remote access/email can be regularly monitored and any misuse will be reported to the Headteacher and or the Online Safety Team.
- The online safety team will meet termly to discuss and review our online safety protocols.

Communicating the Policy

This policy is available for parents, staff and pupils to access online via the school website. It is also accessible to staff on the staff portal. Rules relating to the school code of conduct when online and online safety guidelines are displayed around the school. Online safety is integrated into the curriculum in any circumstance where the internet or technology are being used, as well as during PHSE lessons where personal safety, responsibility and development are discussed.

Managing Information Systems

The school is responsible for reviewing and managing the security of the computers and

internet networks and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as practically possible, against viruses, hackers, and other external security threats. The IT coordinator, the school's external Internet Security Company (Beebug) and Head of ICT will review the security of the school information systems and users regularly, and virus protection software will be updated regularly. Safeguards that the school takes to secure our computer systems are:

- Ensuring that all personal data sent over the internet is encrypted
- Ensuring that unapproved software/apps are not downloaded to any school devices and alerting users of this.
- Files held on the school network will be regularly checked for viruses.
- Enforcing the use of user logins and passwords to access the school network

Please see the school Data Protection Policy for further information on data security.

Emails

The school uses email internally for staff and pupils, and externally for contacting parents, and is an essential part of school communication. It is also used to enhance the curriculum by:

- Providing immediate feedback on work, and requests for support where it is needed.
- Initiating contact and projects with other schools nationally

Staff and pupils are aware that school email accounts should only be used for school related matters. This is important for confidentiality. The school has the right to monitor emails and their contents.

ERS also communicates with parents via Teachers2Parents to email addresses registered with us for this purpose.

School Email Accounts and Appropriate Use

Staff Emails

- Staff will only use official school provided email accounts to communicate with pupils, parents or carers. Personal email accounts must not be used for school related business and should not be accessed during school hours.
- Staff will inform their line manager or member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- The forwarding of chain messages is not permitted in school.

Pupil Emails

Pupils should be aware of the following when using email in school, and will be taught to follow these guidelines through the ICT curriculum and PHSE lessons and in any instance where email is being used within the curriculum or in class:

- In school, pupils should only use school approved email accounts
- Social emailing is restricted
- Pupils should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They

should not attempt to deal with this themselves.
- Pupils must be careful not to reveal any personal information over email or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.

School Website.
The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, pupils and staff for keeping up-to-date with school news and events, celebrating whole school achievements and personal achievements, and promoting school projects.
The website is a public domain and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or pupils will be published and details for contacting the school will be for the school office only

Parents Pages
As part of our drive to improve communication and content sharing between the school and parents we have an additional secure webpage called Parents Pages. Login details for Parents Pages are made available to all parents.

Safe use of pupil's photographs/videos and work
Under the General Data Protection Regulation 2018 images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers will be asked to sign a photography consent form. For students aged 13 and above their explicit consent is also required. Parents are contacted annually for consent. Photograph files and system management photos are removed/destroyed once a pupil leaves the school.
The school has a Go Pro camera which is used in some teaching and therapy and also during offsite residential trips. Parental and pupil (aged 13 and above) consent is obtained before recording any pupil with the Go Pro. Videos recorded during therapy are filed on the therapist's school computer which is password protected. All videos on file are destroyed by the therapist when the pupil leaves the school, unless parental consent has been given to use the video for in house training purposes. A consent form is filed by the therapy department.
For subjects/activities and events that may be filmed, such as PE, Sports Day and Speech Day, the video is not kept after the pupil has left the school, unless used for examination subjects, when it will be kept for 5 years after the child has left the school. All videos are stored securely on password protected computers by the relevant department.

Social Networking, Social Media and Personal Publishing
Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging. These online forums are the most obvious sources of inappropriate and harmful behaviour and where pupils are potentially more vulnerable to content, contact and conduct issues. It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online. Pupils are not allowed to access social media sites in school. There are restrictions, via filtering, on the use of these sites in school that apply to both students and staff.

- Although responsibility for a pupil's use of any social media site is a parental responsibility and should take place out of school hours and offsite, pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. Parents are advised regularly on age restrictions for the various social sites.
- More generally they are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online, whether in school or outside.
- Any sites that are to be used in class are limited and monitored, and will also be risk assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Safe and professional behaviour of staff online is discussed at staff induction.

Mobile phones and Personal Devices

While mobile phones and personal communication devices are commonplace today, their use and the responsibility for using them should not be taken lightly. Possession and use of these devices can:

- Make pupils and staff more vulnerable to cyberbullying
- Allow for access to inappropriate internet material
- Be a distraction in the classroom
- Lead to risk of damage, loss or theft
- Lead to child protection, bullying and data protection issues when the device has an integrated camera

The school takes measures to ensure mobile phones are not used in school and all pupils must hand their phones in at registration and collect them at the end of the day. Pupils in years 12 and 13 may have occasional use of their phones during the school day but are not allowed to use them for social media. Phones must be turned off when leaving any transport to school and not turned on again until boarding transport at the end of the day.

The school will not tolerate cyber bullying against either pupils or staff. Sending inappropriate, suggestive or abusive messages is not allowed and anyone who is found to have sent a message of such content will be disciplined. For more information on the school's disciplinary sanctions see the school behaviour policy.

A member of the senior leadership team may search a device if there is reason to believe that there may be evidence of harmful or inappropriate use.

Any pupil who brings a mobile phone or personal device into school is responsible for its safety. The school will not take responsibility for personal devices that have been lost, stolen or damaged.

Images or files should not be sent between mobile phones when on school transport.

Pupils who breach school policy relating to the use of personal devices will be disciplined in line with the school's behaviour policy. Their mobile phone may be confiscated.

Pupils are not allowed to take mobile phones or personal devices into examination rooms with them. If a pupil is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining board and may result in ramifications at the discretion of the examination board.

Under no circumstances should staff use their own personal devices or personal contact details to contact pupils or parents either in or out of school time.

Any communication received from a pupil who may have obtained a staff personal phone

number should be ignored and reported to the Headteacher as soon as possible.
Staff are not permitted to take photographs or videos of pupils. School equipment will be used when photos or videos are being taken as part of the school curriculum or for a professional capacity. Staff personal mobile phones should be switched off or on silent during school hours.

Online risks – see also our safeguarding policy
Children and young people may experience several types of abuse online:
Bullying/Cyber bullying
Emotional abuse – including blackmail and pressure to comply with sexual requests via technology
Sexting
Sexual abuse
Sexual Exploitation
Children can also be groomed online and the perpetrators may use online platforms to build a trusting relationship with the child in order to abuse them either online or face to face.
Children can also be revictimized, (experiencing further abuse) when abusive content is recorded uploaded or shared by others online. This can happen if the original abuse happened online or offline**.**

Cyberbullying
The school takes cyber bullying in or out of school very seriously. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, staff and members of the public and any intentional breach of this will result in disciplinary action. Strategies to prevent and tackle cyberbullying can be found in the school anti bullying policy.
If an allegation of bullying occurs, the school will:

- Take it seriously
- Act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider to identify the bully.
- Record and report the incident.
- Make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a group. It is important that children who have harmed another pupil, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.
- If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published and the service provided may be contacted to do this if they refuse or are unable to remove it. They may have their internet access suspended in school.
- Repeated bullying may result in a fixed term exclusion.

Youth-produced sexual imagery (Sexting) and Safeguarding Procedures – See also the school's Safeguarding policy

This refers to the creating and sharing of sexual imagery by young people. Creating and sharing sexual photos and videos of under-18s is illegal and therefore causes the greatest complexity for schools and other agencies when responding. It also presents a range of safeguarding risks which need careful management.

The term 'youth-produced sexual imagery' (YPSI) is now used instead of 'sexting.' This is to ensure clarity. The types of incidents which this covers are those where a person under the age of 18:

- creates and shares sexual imagery of themselves with a peer under the age of 18
- shares sexual imagery created by another person under the age of 18 with a peer under the age of 18 or an adult
- is in possession of sexual imagery created by another person under the age of 18

As it is a criminal offence to possess, distribute, show and make indecent images of children, any disclosure of information about an incidence of YPSI will always be taken very seriously by the School. The Sexual Offences Act 2003 (England and Wales) defines a child, for the purposes of indecent images, as anyone under the age of 18.
When an incident involving youth-produced sexual imagery comes to the School's attention:

- the incident MUST should be referred to the DSL as soon as possible
- the DSL will hold an initial review meeting with appropriate school staff
- there will be subsequent interviews with the young people involved (if appropriate)
- parents will be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm.

At any point in the process if there is a concern that a young person has been harmed or is at risk of harm, a referral will be made to Children's Social Care and/or the police immediately.
An immediate referral to police and/or Children's Social Care will also be made if at this initial stage:

- the incident involves an adult
- there is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example, owing to special educational needs)
- what is known about the imagery suggests violent content
- the imagery involves sexual acts and any pupil in the imagery is under 13
- there is reason to believe a young person is at immediate risk of harm because of the sharing of the imagery, e.g. the young person is presenting as suicidal or self-harming.

If none of the above applies, then the School may decide to respond to the incident without involving the police or Children's Social Care. However, the School can choose to escalate the incident at any time if further information and/or concerns come to light.

Pupils with SEN
Pupils with SEN have an increased vulnerability to risk online, especially those with language and communication needs or social communication difficulties. Online safety is a fundamental part of our safeguarding responsibilities and a range of differentiated strategies are implemented to enable learners with SEN to access the internet safely and appropriately. Our online safety education is delivered in an age and context appropriate way. This is done by:

- Complex online safety issues to be broken down and explained in greater detail
- Exploring issues in a variety of contexts and approaches
- More examples of safe and unsafe practices
- Constant reinforcement and repetition of key safety messages
- Differentiated teaching resources and materials.
- Help to develop resilience and to know how to seek help

The school's DSLs work with the Lead SENCo and other relevant staff to develop and review online safeguarding policies, ensuring that the specific needs and requirements of learners with SEN are met. If individual learners are identified with specific online safety concerns, these can be incorporated into the pupil's EHC plan.

Managing Emerging Technologies
Technology is progressing rapidly, and new technologies are emerging all the time. The school will risk assess any new technologies before they are used in school and will consider any educational benefits that they might have. The school keeps up to date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

Protecting Personal Data
ERS believes that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole school and individual progress. The school collects personal data from pupils, parents and staff and processes it to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision.
We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary. The school will keep parents fully informed of how the data is collected, what is collected and how it is used. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progress of our school body to ensure that we are doing all we can to support both staff and students.
Please see the school's Data Protection Policy, Data Retention Policy and Privacy Notices for further information.
The school's Data Protection Officer is Ms Sarah Vest.

Passwords and Password Security
Logins and passwords are obtained via the IT & Network coordinator. Pupils from Year 10 upwards can set their own passwords. The IT & Network coordinator can access and change all passwords. The IT & Network coordinator manages password updates and

security as necessary and reviews them annually.

Webcams & Video Conferencing
The school use of applications allowing on-line conferencing for lessons was introduced at the time of the Covid-19 pandemic. These are not a part of everyday teaching but remain available in the event of any further school closures. Staff and parents are made aware that individual conversations with pupils will only take place with an adult always present. Pupils and parents are told that no recording of subject sessions or screen-shots are allowed and that the schools disciplinary procedures will be used and access removed from the pupil if this occurs.
Other platforms such as Google Classroom are also available and similar rules of correct internet use are in place and enforced.

Parental Involvement
We believe that it is essential for parents/ carers to be fully involved with promoting e-safety both in and outside of school and also to be aware of their responsibilities. We consult and discuss e-safety with parents/ carers and seek to promote a wide understanding of the benefits and associated risks related to ICT. Parents are regularly informed via the Teachers2Parents system and or The Egerton of online safety tips and risks.

Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school. Pupils sign an Acceptable ICT Use document in lessons and this is kept on file.

Support links:

Anti-Phishing working group – (https://apwg.org/)

UK safer internet Centre – advice for young people to help stay safe (https://www.saferinternet.org.uk/advice-centre/young-people)

Internet Watch Foundation (can remove child sexual abuse online images and videos and offers a place for them to be reported anonymously) https://www.iwf.org.uk/

NSPCC Helpline to support potential victims of sexual harassment and abuse in education settings is 0800 136 663

Policy approved by: Jon Reynolds
(on behalf of Governing Body)
Date: 30.09.25

Next Review (latest):September 2026

Egerton Rothesay School

POLICY ADDENDUM to Acceptable Use Policy

Pupil Agreement for Online Learning from Home

(In case of any reintroduction due to future pandemics)

We are aiming to keep your access to learning and teaching open through a difficult time and staff will be working hard to provide you with learning sessions via the online systems Zoom, Microsoft Teams and Google Classroom.

We are asking that all pupils agree to this Online Learning Agreement, which is a document that outlines how we expect you to behave when you are learning online.

School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything you do on a school device or using school networks/platforms/internet may be viewed by one of the staff members who are here to keep you safe. You should not behave any differently when you are out of school or using your own device or home network.

The points listed below should be followed at all times and can be summarised as follows:

"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

What am I agreeing to?

1. To ensure that my studies are not disrupted because I am temporarily working away from school, I give permission for my school email to be used by my teachers for teaching and learning purposes.

2. I will treat myself and others with respect at all times; when I am online or using a device, I will treat everyone as if I were talking to them face to face in a classroom.

3. The messages I send, or information I upload, will always be polite and sensible. I understand that all messages I send reflect on me and the school.

4. Even though I am working outside the classroom, I will aim to be positive and creative, to learn and share, to develop new skills and to prepare for the future.
5. I will choose a sensible place to work from – ideally a living room - and I will dress appropriately for my lessons as I would do at school.

6. I will make sure that I have all the tools I need in advance, so that I do not have to leave my desk and interrupt the flow of the lesson.

7. I will be at my pre-arranged session on time.

8. I will complete exercises as directed by my teacher and upload completed work to meet the deadlines set by my teacher.

9. I understand that my online lessons will be monitored by senior leaders from the School.

10. I understand that Google Classroom is a closed school system open to me through the school's Google account and is limited to me, the staff and my fellow pupils. I should not invite any guests from outside the School to join the system through the use of my login details. This also applies to the online platforms 'Zoom' and 'Microsoft Teams'.

11. I will not under any circumstances provide my login details to anyone else. The system is fully secured and my activity on the system can be monitored.

12. I can share work with other pupils in my class but I should let my teacher know who else I am working with.

13. I understand that websites, blogs, videos and other online information can be biased and misleading, so I will need to check sources.

14. I will not download copyright-protected material (text, music, video etc.), and I will avoid plagiarism (copying someone's else's work such as Cut and Pasting from the internet).

15. I will not browse, download, upload, post, share or forward material that could be considered offensive, harmful or illegal. If I accidentally come across any such material I will report it immediately to my teacher.

16. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will never open a file, hyperlink or any other attachment.

17. I will not share my or others' personal information that can be used to identify me, other students or my teachers on any online space, unless a trusted adult has given permission or reviewed the site.

18. I will never take secret photos, recordings or videos of teachers or other students. I MUST NOT screen shot while online with any teacher or other pupil. I will not record any of the sessions or upload any part of them to any social media site or anywhere on the internet.

19. I will never say, text or post anything that could hurt or embarrass another person. I will never use the internet to bully anyone.

20. I will join the sessions at the times I am given and if I am unable to join the session for any reason e.g. through ill health, I will let my teacher know in advance.

~~~~~~~~~~~~~~~~~~~~~~

I have read and understand these rules and agree to them.

Date:
~~~~~~~~~~~~~~~~~~~~~~

Egerton Rothesay School
Acceptable Use of ICT Agreement- Poplar Pupils
(e-Safety Rules)

- I will only use ICT in school for school purposes.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files. I will not look at, alter or delete other people's work or files without their permission.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-Safety.

To Parents of pupils in Poplar
(Date)

Dear Parent

ICT, including the internet, learning platforms, e-mail and mobile technologies, has become an important part of learning in our school.

We aim for all our pupils to be safe and to behave responsibly when using any ICT. It is essential that pupils are aware of eSafety and know how to stay safe when using any ICT.

With this letter you should receive a copy of our 'Acceptable Use of ICT Agreement'. Please read and discuss this agreement with your child and then sign and return the confirmation slip below. If you or your child have any concerns or questions regarding the agreement, please contact either your Base Leader, their class teacher or me.

Yours sincerely

Head of ICT

✂----------

Egerton Rothesay School
Acceptable Use of ICT Agreement

We have read and discussed the school's Acceptable Use of ICT Agreement.

……..... (pupil name) agrees to follow the e-Safety rules within the agreement and to support the safe and responsible use of ICT at Egerton Rothesay School.

Parent Signature ……

Child's Class…..…… Date …..……

Egerton Rothesay School
Acceptable Use of ICT Agreement- Senior School Pupils
(e-Safety Rules)

- I will only use ICT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network/ Learning Platform with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of pupils and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of the Headteacher.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring the school into disrepute.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.

To Parents of pupils in Senior School
(Date)

Dear Parent

ICT, including the internet, learning platforms, e-mail and mobile technologies, has become an important part of learning in our school.

We aim for all our pupils to be safe and to behave responsibly when using any ICT. It is essential that pupils are aware of eSafety and know how to stay safe when using any ICT.

With this letter you should receive a copy of our 'Acceptable Use of ICT Agreement'. Please read and discuss this agreement with your child and then sign and return the confirmation slip below. If you or your child have any concerns or questions regarding the agreement, please contact either their Base Leader, Form Tutor or me.

Yours sincerely

Head of ICT

✂----------

Egerton Rothesay School
Acceptable Use of ICT Agreement

We have read and discussed the school's Acceptable Use of ICT Agreement.

……..... (pupil name) agrees to follow the e-Safety rules within the agreement and to support the safe and responsible use of ICT at Egerton Rothesay School.

Parent Signature ……..…….……..……

Pupil Signature……

Form …… Date …...……

Smile and Stay Safe Poster

e-Safety guidelines to be displayed throughout the school

SMILE and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'.

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.