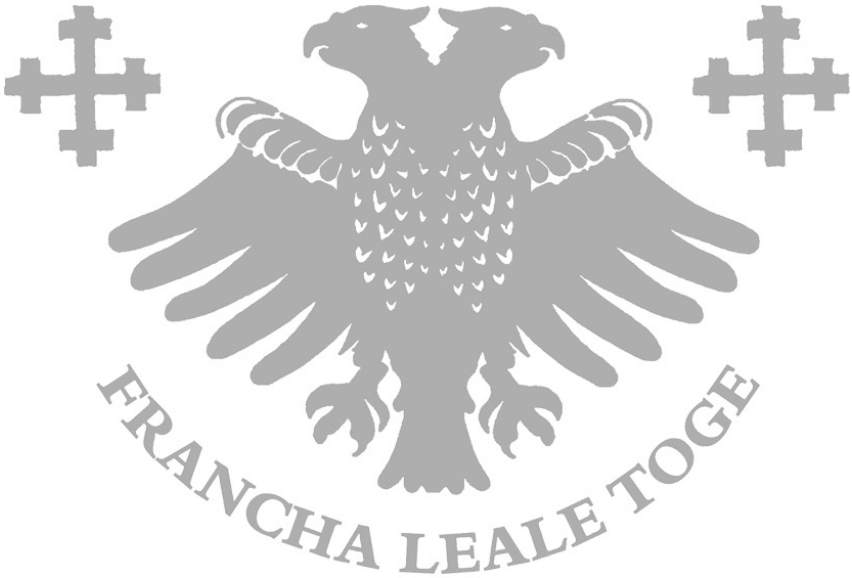
Godolphin & Latymer

Redcliffe Gardens School

Online Safety Policy

Reviewed: SL/PA August 2020
Minor amendment: April 2021
Prep School Committee: June 2021

Next review by: September 2021



This policy applies to the whole school including the EYFS.

1. Introduction

1.1. Online safety encompasses all internet technologies and devices that connect to the online world. The purpose of this policy is to promote:

- Responsible use of online technology by all staff and students, encouraged by education and made explicit through published policies
- Sound implementation of Online Safety policy in both administration and curriculum, including secure school network design and use
- Safe and secure internet access with a secure and safe filtering and monitoring system
- Protection of personal and sensitive information (data)
- Responsible use of any online remote teaching platforms that are used to support learning.

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

1.3. This policy should be read alongside other policies including those for Computing, Data Protection, Safeguarding and Child Protection, and Use of Social Media. This Online Safety policy has been agreed by senior leadership and approved by Governors. The policy and its implementation will be reviewed annually; senior leadership and the Online Safety and Computing coordinator will regularly monitor compliance and review the policy in light of any significant new developments in the use of the technologies, data protection, new threats to online safety or incidents that have taken place.

2. Education – Pupils

2.1. Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build resilience.

2.2. Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum, which should be broad, relevant and provide progression, with opportunities for creative activities, will be provided in the following ways:

- A planned online safety curriculum will be provided as part of Computing and PSCHEE lessons, covering both school and home safe use
- Key online safety messages will be reinforced during assemblies
- Online Safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year
- Pupils will be taught in all lessons to be critically aware of the content they access online and be guided to validate the accuracy of information.

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils will be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils will be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use
- If internet research is set for homework, specific sites will be suggested which have previously been checked by the teacher. It is advised that parents re-check these sites and supervise this work. Parents will be advised to supervise any further research
- Pupils are made aware of the 'Think then Click' policy (see Appendix 2) and what to do If they come across unsuitable material during internet searches
- The School will supervise all access to internet resources (where reasonable) and pupils will not be allowed to use devices if there is not a supervisor present
    - At *Key Stage 1* all pupils' access to the internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
    - At *Key Stage 2* all pupils will be supervised when using the internet. Pupils will use age- appropriate search engines and online tools; and online activities will be teacher-directed where necessary.
    - During remote learning all pupils will be supervised when using the internet by parents or guardians.

- The School subscribes to Britannica School and Britannica Images; all teachers, parents and pupils are encouraged to use the site as their first source of information when completing research or searching for images
- The School recommends the use of safe web searching websites
    - Ask Kids (http://www.askkids.com
    - Safe Search - https://www.google.safesearchkids.com
    - YouTube kids - https://youtube.com/kids

3. Education – Parents / Carers

3.1. Parents and carers play an essential role in the education of their children and in the monitoring of their children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

3.2. The school will therefore seek to provide information and awareness to parents and carers through:

- Online Safety presentations
- List of suggested websites and apps posted on school website
- Provision of the Acceptable Use Policy (See Appendices Three and Four).

3.3. Parents will be provided with a Privacy Notice that describes how the School holds and uses their own and their child's personal data.

3.4. Parents will be responsible for monitoring their children's use of the internet whilst online at home and during remote learning sessions.

4. Education & Training – Staff / Volunteers

4.1. It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows

- A formal online safety training will be provided to staff annually
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school's Online Safety Policy, and the Acceptable Use of ICT for Staff (in the Employment Handbook).
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings or on INSET days.
- The Online Safety Coordinator will provide guidance to individuals as required.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff will receive regular training and updates on the protection of personal information.
- Staff are provided with access to relevant guidance and training to enable remote learning as required.

5. Technical – Equipment, filtering and monitoring

5.1. The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

5.2. It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

5.3. Technical measures include the following:

- There will be regular reviews and audits of the safety and security of school technical systems
- All users will have clearly defined access rights to school technical systems and devices.
    - Staff will be provided with a username and secure password by the Computing Co-ordinator who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password
    - Pupils will have class logons
- Internet access is filtered for all users.
    - IT Lab, our current IT provider, employs WEB BLOCKER

- Illegal content is filtered by WEB BLOCKER; WEB BLOCKER actively employs the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- There is a clear process in place to deal with requests for filtering changes
    - Staff may request that websites be removed from the blacklist by providing the online safety coordinator with the website.
    - The online safety coordinator will verify the website is safe and send a request to the IT provider to whitelist the website.
    - The online safety coordinator will keep a record of requested websites for administration to review.
- The internet filtering settings ensure that children are safe from terrorist and extremist material when accessing the internet.
- The Senior Leadership team and Online Safety coordinator regularly monitor and record the activity of users on the school IT systems and users are made aware of this in the Acceptable Use Agreement.
    - The School uses Securus software to monitor internet use on pupil laptops, iPads and staff computers located in classrooms (where children may have access to them)
- Reporting Incidents (Staff):
    - All staff must report any actual or potential technical incidents or security breaches to the Head, the Designated Safeguarding Lead, or the Online Safety Coordinator in the first instance that they occur or that the member of staff becomes aware of them.
    - Staff must isolate the device involved in the incident and not make any changes to the device (i.e. leave the iPAD exactly as it is, do not close the webpage or turn off the computer)
    - The Online Safety Coordinator will keep a log of all instances (see Appendix 3).
    - The Online Safety Coordinator and the SLT will investigate and decide on an appropriate course of action in each instance.
        - E.g. A block will be created on a website that is deemed not appropriate
    - If an incident does occur children are taught these key rules:
        - Minimise the image or window immediately – Do not close the page!
        - Children report incident to teacher
- The IT provider (IT Lab) employs appropriate security measures to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Guest Access: The provision of access to guests will be addressed in the following way
    - Trainee Teachers- The Computing Coordinator will have IT lab create a unique login for the teacher which will be deactivated at the end of their period of training at the School.
    - Supply Teachers – The Computing Coordinator will provide supply teachers with a temporary access login and password.
    - Other guests will be provided with the WIFI password, should they require it, but not granted access to the school network.
- The ability to install programs is restricted to protect the school computers and prevent downloading of unsuitable content. Staff/pupils who wish to download

programs must seek permission from the Computing Coordinator who will ensure the content is suitable and safe.

- Staff should use the school's secure drives for the storage of all data; staff may access the server from home using their unique VPN credentials
- Staff must use encrypted data USB if they need to transfer files that contain personal information about pupils or other staff
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

6. Use of Digital and Video Images

6.1. The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Pupils work can only be published with the permission of the pupil and parents or carers.
- The Headmistress will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Parents/Carers will be asked to sign a Use of Digital/Video Images consent form at the beginning of every year.
- Teachers should not live-stream lessons from their homes, nor engage in any video-calling unless in exceptional circumstances, with the parent(s) and the Head Teacher's permission.

7. Mobile Technology, Communications and Email

7.1. A wide range of rapidly developing communications technologies has the potential to enhance learning and teaching. The School provides staff and pupils with access to iPads and laptop computers for this purpose. The school will adhere to the following guidelines regarding mobile technology and pupil access:

- The school Acceptable Use Agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies
- The school allows staff to use personal and school owned devices to access the Internet. The network may be accessed using school owned devices whilst at school, or via the individual's VPN credentials.
- Visitors to the school may be granted access to the Internet at the discretion of the staff member hosting the visitor, but not the network.
- Personal mobile devices for pupils are not permitted to be used in school. Any devices brought to school will be confiscated by the teacher/head and returned directly to the parent/carer at the end of the school day.

7.2. When using communication technologies the school considers the following as good practice:

- The official school email service (iSAMS) may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the Head teacher, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class/group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with

inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- Any contact between pupils and teachers should only be through a platform specified by the school and not through personalised accounts open to public viewing, comments or sharing.
- 'Live' lesson recording for use during remote learning should be made in a safe, neutral setting and conducted in a professional manner, including appropriate attire.

8. Data Protection

8.1. The School will ensure that we maintain confidentiality of records about staff and children, with access only available to those who have a right or a professional need to see them. Parents or carers must be given access to records about their child, provided that no relevant exemptions apply to their disclosure under the Data Protection Act and described in the Privacy Notice.

8.2. All personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations. Please refer to the school's Privacy Notice for Parents and Pupils or Privacy Notice for Staff.

8.3. When using technology, pupils and staff will:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- Delete personal data inline with the Data Retention Policy.

9. Responding to Incidents of Misuse

9.1. It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

9.2. **In the event of suspicion, all steps in this procedure should be followed:**

- **Report the suspicion** to at least two of the three following individuals: the Head, Deputy Head or Online Safety/Computing Coordinator. The report should never be investigated alone; this is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

- Before any investigation into the misuse occurs, contact IT Lab to inform them of the intended investigation and the computer with which the investigation will be carried out on. They will then be able to monitor and record the sites and content visited (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (see Appendix 4). **(except in the case of images of child sexual abuse – see below)**
- Once this has been completed and fully investigated the group will judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority
    - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- **Staff must always remember to isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

9.3. It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

10. Cyber-bullying

10.1. Pupils will not be given access to social media whilst at school and will not have access to personal mobile devices. Lessons will be taught on how pupils can keep themselves safe, as well as not become perpetrators of, cyber-bullying. Pupils will discuss the Pupil Acceptable Use Agreement (See Appendix 1) and Think Then Click policy (see Appendix 2) with their teachers and parents. The school will investigate all incidents of cyber-bullying that occur involving the pupils. For more information on the school's policy towards incidents of cyber-bullying, see the Anti-Bullying Policy.

11. Additional Resources

www.thinkuknow.co.uk
www.disrespectnobody.co.uk
www.saferinternet.org.uk
www.internetmatters.org
www.pshe-association.org.uk
https://educateagainsthate.com/

https://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

Recommended safer search engines for children are as follows:

- http://www.bbc.co.uk/cbbc/find/ - range of information can be accessed
- www.askkids.com - this is excellent for images and information
- www.kidsclick.org - encyclopedia, images, facts etc

APPENDIX 1 – Pupil and Parent Acceptable Use Agreements

Godolphin and Latymer Redcliffe Gardens School Pupil Acceptable Use Agreement

(EYFS, KS1 & Y3)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers or iPads
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable 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

Signed (child): .....

Signed (parent): .....

Godolphin and Latymer Redcliffe Gardens School Pupil Acceptable Use Agreement

(Years 4-6)

Acceptable Use Policy Agreement
I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will be aware of "stranger danger", when I am communicating online.
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I will act as I expect others to act toward me:

- I will respect others' electronic work and property.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person who sent the email. I will ask a teacher/parent if I'm unsure.

When using the internet for research or recreation, I recognise that:

- I will not copy others' work and present it as my own.
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that not all information on the internet is truthful.

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

- I understand that it my responsibility to treat all other users of internet services respectfully, at home and at school and,
- I understand that if I do not follow our online safety rules my access to ICT will be revoked.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Name of Pupil: …….. Form: ……..

Pupil Signature: …….. Date: ……..

Parent Signature: ……

Godolphin and Latymer Redcliffe Gardens School Parent Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Student Acceptable Use Policy is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.
Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work. Please also review the Student Acceptable Use Policy with your child and sign it.

Parent Name: ..... Pupil Name.....

As the parent/carer of the above pupil, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

I understand that the school cannot monitor the use of the internet whilst providing remote teaching. All content uploaded to lessons by teachers will be age appropriate but further online content that is researched by a pupil should be monitored by parents. We recommend adjusting your online filters/content blocking software appropriately.

Signed: .....

Parent Acceptable Use Remote Learning Agreement COVID-19

FOR PARENTS AND THEIR CHILDREN WHILST STUDYING AT HOME

1. *I have read and explained to my child this Acceptable Use of Technology Policy (AUP).*

2. *I have further explained:*

   a. *The aim of the AUP is to help keep children safe on-line.*
   b. *That School systems and devices may be monitored*
   c. *Monitoring will be proportionate and will take place for safeguarding purposes and in accordance with data protection, privacy and human rights legislation.*
   d. *I am responsible for the nature and content of materials accessed on the internet whilst my child is studying at home.*
   e. *The importance of safe online behaviour.*
   f. *No images, video, sounds or text should not be uploaded that may risk the safety or offend any member of the school.*
   g. *The school will contact me if they have concerns about any possible breaches of the AUP or they have any concerns about their (my child's) safety.*
   h. *I will inform the school or other relevant organisations if I have concerns over their (my child's) or other members of the schools online safety.*

3. *We understand that my child will:*

   a. *Use our devices whilst studying at home.*
   b. *If using School devices, these will only be used for school study.*
   c. *Ask permission from an adult before going on-line to complete school work.*
   d. *Only use school authorised settings, websites, search engines and filters.*
   e. *Keep personal information safe and private when on-line including passwords.*
   f. *Always tell me if they have any worries or feel uncomfortable when on-line.*
   g. *Not access or change other people's files, information or status.*

4. *I understand that if my child or I do not abide by the above conditions that action may be taken by the School. This could include sanctions being applied in line with school policies and, if a criminal offence has been committed, the police being contacted.*

5. *I know that I can speak to the Designated Safeguarding Lead (DSL) or the Head or my child's teacher if I have any concerns about on-line safety.*

Child's Name ……

Child's Year …….. Class …… Date of Signature ……..

Parent / Carers Name …….. (as appropriate)

Parent / Carers Signature …….. (as appropriate)

APPENDIX 2 – 'Think then Click' Rules

Lower School:

Redcliffe Gardens Lower School

'Think then Click'
These rules help us to stay safe when using technology

We always ask an adult before we use the computers or iPads

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We always tell the teacher or another adult if we see something that upset us on the screen.

We take care of the computers and other equipment.

We discussed these rules with our teacher and understand them

Date _____

Upper School:

Redcliffe Gardens Upper School

'Think then Click'

Online Safety Rules for Upper School

- We ask permission before using the computers or iPads.
- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately minimize any webpage we are unsure about and tell an adult.
- We only e-mail/chat/message/accept as friends, people an adult has approved.
- We send e-mails/messages/texts/comments that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails/messages/texts sent by anyone we don't know.
- We do not take or distribute pictures of people without their permission.
- We remember the 'Digital Tattoo' when emailing/texting/chatting/posting - everything we do using electronics can never be completely deleted.

We understand and agree to these rules

Date _____

APPENDIX 3 – Incident Log

Reporting Log Group:						
Date	***Time***	***Incident***	***Action Taken***		***Incident Reported By***	***Signature***
			What?	***By Whom?***		

APPENDIX 4

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group: .....
Date: .....
Reason for investigation: .....
.....
.....
.....

Details of first reviewing person
Name: .....
Position: .....
Signature: .....

Details of second reviewing person
Name: .....
Position: .....
Signature: .....

Name and location of computer used for review (for web sites)

.....
.....

Web site(s) address / device	***Reason for concern***

Conclusion and Action proposed or taken
