

# E-Safety Policy



This policy has been written with the support of the wider school community and it is implemented with due regard to the school’s mission statement.

**‘Inspire, challenge and support all through faith.’**

- Governors are kept informed of pertinent legislation changes and ISI updates through the Curriculum sub-Committee reports.
- Staff are kept informed of pertinent legislation changes and ISI updates during weekly briefing.

<b>Version Control</b>	
Governor Co-ordination:	<b>Curriculum Committee</b>
Approved by Governors:	<b>Summer 2015</b>
Review Cycle:	<b>Bi-Annual</b>
Next Review Date:	<b>Summer 2020</b>
Last Amended:	<b>September 2018</b>
Latest ISI Update Check:	<b>September 2018</b>
See also - Health & Safety Policy	



# **Runnymede St Edward's School: Mission Statement**

## **'Inspire, Challenge, Support through Faith'**

### **Children's Mission:**

Into your hands Lord, we put each day  
all that we do and all that we say

### **Child Protection Statement:**

Runnymede St Edward's School is committed to safeguarding children and promoting children's welfare and expects all staff, governors, volunteers and visitors to share this commitment and maintain a vigilant and safe environment. Everyone has a responsibility to act without delay to protect children by reporting anything that might suggest a child is being abused or neglected. It is our willingness to work safely and challenge inappropriate behaviours that underpins this commitment. The school seeks to work in partnership with families and other agencies to improve the outcomes for children who are vulnerable or in need.

Runnymede St Edward's School follows guidelines laid down by the **Liverpool Safeguarding Children Board** (LSCB: [www.liverpoolscb.org](http://www.liverpoolscb.org) 2018) and **Keeping Children Safe in Education** ([www.gov.uk](http://www.gov.uk) 2018)

### **School Aims:**

#### **Faith**

To encourage and foster the spiritual growth of all and to make prayer an integral and enjoyable experience in our daily life.

#### **Individual Opportunities for Learning and Growth**

To provide experiences that broaden, enrich and extend the skills, talents and values of each member of the school community. We are an inclusive school and pupils with additional needs or for whom English is an additional Language are fully supported to enable them to achieve their potential.

#### **Relationships**

To provide a safe, caring and welcoming environment within which all are treated with respect, courtesy and kindness. Runnymede St Edward's School upholds British values and encourages respect for all.

#### **School and Wider Community**

To foster a spirit of co-operation and friendship between home, school and the wider community.

Runnymede St Edward's School is built on the tradition of our founders, the Congregation of Christian Brothers. Based on their vision, Runnymede is a place in which individuals can develop fully, contributing as happy and caring members of a school community. Children's unique talents are valued, and they learn to live as well-mannered, self-disciplined and confident individuals.

**For a detailed School Mission Statement please refer to the Mission Statement page of our website**



## 1. Introduction

- 1.1. This policy has been developed as a result of a process of consultation. It has been agreed by senior managers and approved by Governors.
- 1.2. It is a statement of the aims, principles and strategies for the safe use of Internet and related technologies at Runnymede

## 2. Philosophy

- 2.1. E-safety means electronic safety. It is concerned with the protecting of young people in the digital world and ensuring they feel safe when accessing new technology. They protect from unsuitable material and prohibited activities taking place online effecting both adults and children.
- 2.2. Everyone has a role to play in empowering children to stay safe while they enjoy the new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world." Byron Report – a review. ( 2010).
- 2.3. Runnymede St Edward's recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use.
- 2.4. Our approach is to implement appropriate safeguards within the school while supporting staff and learners to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. In furtherance of our duty to safeguard learners, we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care. This e-safety policy should be read alongside other relevant policies i.e. Safeguarding, Social Media, Anti Bullying, Disciplinary and Health and Safety.

*"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.*

*To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom."* DfES, eStrategy 2005

- 2.5. This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

## 3. Aims

- 3.1. The philosophy of 'empowering children to stay safe' includes aims that children are:-
  - safe from maltreatment, neglect, violence and sexual exploitation
  - safe from accidental injury and death
  - safe from bullying and discrimination
  - safe from crime and anti-social behaviour in and out of school
  - secure, stable and cared for.

## 4. Scope of the Policy

- 4.1. This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school COMPUTING AND ICT systems, both in and out of school.
- 4.2. The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the school site and empowers members of staff to impose disciplinary



penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

**4.3.** The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

## **5. Whole school responsibility for the safe use of Computing and ICT**

### **5.1. What does this mean? We need to:**

- Regularly reinforce e-safety messages and keep policies updated (with input from **all** stakeholders).
- Ensure that **all staff** have some understanding of e-safety issues and that they are regularly updated.
- Provide pupils with a progressive curriculum which delivers appropriate guidance and advice embedded across a range of subjects where appropriate.
- Offer support to parents and the wider school community.
- Find opportunities to provide practical support for pupils – for example with privacy settings and helping to manage their online reputation.
- Establish a Digital Council.
- Provide a staff reference copy of - Internet Safety for Prep Schools – Karl Hopwood

**5.2.** E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The head teacher ensures that the Policy is implemented and compliance with the Policy monitored.

## **6. Responsibilities**

**6.1.** The responsibility for e-Safety has been designated to Mr B Slater, Headteacher.

**6.2.** Our school **e-Safety Co-ordinator** is the Computing Coordinator, who ensures they keep up to date with e-Safety issues and guidance through organisations such as Internet Watch Foundation (IWF) and The Child Exploitation and Online Protection (CEOP)<sup>1</sup>. The school's e-Safety coordinator also ensures the Head, senior management and Governors are updated as necessary.

**6.3. Governors** need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance <sup>2</sup> on e-Safety and are updated at least annually on policy developments.

**6.4. All teachers** are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials

---

<sup>1</sup> <http://www.ceop.gov.uk/>

<sup>2</sup> Childnet – [www.childnet.com](http://www.childnet.com)

[www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

UK Safer Internet Centre – [www.saferinternet.org.uk](http://www.saferinternet.org.uk)

[www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/](http://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/)



## 7. The Technologies

7.1. Computing and ICT in the 21<sup>st</sup> Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging (<http://www.msn.com>, <http://info.aol.co.uk/aim/>) often using simple web cams or mobile devices
- Blogs (an on-line interactive diary)
- Podcasting (radio/audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular ones include: Instagram, [www.myspace.com](http://www.myspace.com), [www.piczo.com](http://www.piczo.com), [www.bebo.com](http://www.bebo.com), <http://www.hi5.com>)
- Video broadcasting sites (Popular: <http://www.youtube.com/>)
- Chat Rooms (Popular [www.teenchat.com](http://www.teenchat.com), [www.habbohotel.co.uk](http://www.habbohotel.co.uk))
- Gaming Sites (Popular [www.neopets.com](http://www.neopets.com), <http://www.miniclip.com/games/en/>, <http://www.runescape.com/>, [Minecraft](http://www.minecraft.com))
- Music download sites (Popular <http://www.apple.com/itunes/> <http://www.napster.co.uk/> <http://www-kazaa.com/>, <http://www-livewire.com/>)
- Mobile phones/tablets with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

## 8. Accessing the Internet

- 8.1. The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- 8.2. All staff must read and sign the Staff Code of Conduct for Acceptable Internet Use before using the school computing and ICT resource.
- 8.3. For younger children, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on – line materials.
- 8.4. Parents will be asked to sign and return a consent form for pupil access.
- 8.5. Parents will be informed that pupils will be provided with supervised Internet access.

## 9. The Internet and Learning

- 9.1. Digital Literacy is now an integral part of the Computing and ICT curriculum (2014) and our school has incorporated this into our discrete planning.
- 9.2. Younger children should be **offered selected sites rather than the open Internet search**. Older children benefit from the same use of suggested sites and must also be encouraged to evaluate everything they read and to refine their own publishing.
- 9.3. Plagiarism will be discouraged at all times and children will be taught to acknowledge sources in their work.
- 9.4. Pupils will be taught what Internet use is acceptable and what is not, and given clear objectives for Internet use.
- 9.5. These rules are based on Childnet's SMART rules for children:-  
S – stay **safe**, do not give out personal information  
M – Tell an adult if you are thinking of **meeting** someone.  
A –**Accepting** e-mails or open attachments from people you do not know can lead to viruses and unwanted emails.  
R – Information you find on the Internet may not be **reliable** and people may not be who they say they are.  
T- **Tell** a parent, carer or trusted adult if someone or something makes you feel uncomfortable or worried, and if you or someone you know is being bullied online.



9.6. The school internet access is designed expressly for pupil use and includes filtering appropriate to primary school children.

9.7. Other teaching tools include the use of e-safety websites including:

- Think U Know ([www.thinkuknow.co.uk](http://www.thinkuknow.co.uk))
- Grid Club ([www.gridclub.com](http://www.gridclub.com))
- Kidsmart ([www.kidsmart.org.uk](http://www.kidsmart.org.uk))
- Bizzikid ([www.bizzikid.co.uk](http://www.bizzikid.co.uk))
- UK Safer Internet Centre ([www.saferinternet.org.uk](http://www.saferinternet.org.uk))

## 10. E-mail

10.1. E-mail is an essential means of communication for both staff and pupils. Directed e-mail has significant educational benefits when used in projects between schools and children in other countries.

10.2. In addition –

- Pupils may only use approved school e-mail accounts.
- Pupils may not send or check e-mails without the teacher's permission.
- Whole emails can be forwarded via the teacher's e-mail address.
- Pupils must immediately tell the teacher if they receive offensive e-mail.
- Pupils must not reveal personal details, send photographs of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to external organisations should be written carefully and using the school signature.
- The forwarding of chain letters is not permitted.
- The school's administrator account is copied into any emails to and from pupil accounts within school for record purposes only, and children are made aware of this when they're granted access to their accounts.
- Informed parental permission is obtained before setting up new pupil accounts as these are Gmail accounts with restricted access and functionality.
- Pupil email accounts are restricted to internal emails only unless explicit permission is obtained for external emailing.

## 11. Website

### 11.1. Images -

- 11.1.1. Runnymede St Edward's website has been designed to showcase the very best of our school to parents, relatives and friends, our local community and to the world via the Internet. One part of portraying the school will be the inclusion of photographs taken in and around the school, on school visits, at sporting events, during school performances etc. and possibly examples of children's work
- 11.1.2. We believe that photographs of our pupils are a valuable part of delivering an accurate portrait of the school; however we acknowledge that we must adhere to certain restrictions in order to ensure the safety of everyone that we feature on our site. Therefore, the following rules will apply to **all** content that is provided on our site:
- 11.1.3. If a photograph of a child is published it will never be accompanied by the pupil's name unless authorized by the parent in writing.
- 11.1.4. Where possible, pupils will be photographed in groups; however, if a pupil is featured on their own, special permission will be sought from the parents before the image is published on the site.
- 11.1.5. All parents, pupils and staff of Runnymede St Edward's have the right to request that images of themselves or their children are not published on the site. Withdrawal of permission must be made in writing to the School Office and an acknowledgement will be sent by return of post.



## 12. Other

- 12.1. Contact details on the website will include school address, e-mail and telephone number. Staff or pupil personal details must not be published.
- 12.2. No link should be made between an individual and any home address (including simply street names);
- 12.3. The Headteacher will take overall editorial responsibility to ensure that content is accurate and appropriate.
- 12.4. The school must respect intellectual property rights and copyright.
- 12.5. Work can only be published with the permission of pupil and parents.
- 12.6. We believe that the website is fundamentally a positive aspect of our school and the integrity of the school staff in general will ensure that no inappropriate material is published.
- 12.7. If you do have any specific enquiries in addition to the rules listed above then please contact the School Office, Miss L Robinson by phone on 0151 281 2300, email to [contact@runnymede-school.org.uk](mailto:contact@runnymede-school.org.uk) or write to the school address.

## 13. Social Networking (See also Social Media policy)

- 13.1. Examples of social networking sites include- wikis, blogs, MySpace, Facebook, Instagram, Bebo, bulletin boards, chat rooms, instant messaging and many others.
- 13.2. As children can access these at home, advice to children will be supplemented by similar advice to their parents.
- 13.3. School will block access to these sites and others.
- 13.4. Newsgroups will be blocked unless a specific use is approved.
- 13.5. **Pupils** will be advised never to give out personal details of any kind which may identify them and/or their location.
- 13.6. **Pupils** will be advised not to place personal photos on any social network space.
- 13.7. **Parents** will encourage children to use these sites appropriately with respect for others and with due consideration for the privacy of themselves and others. Parents will support the children in understanding the advice they're given about staying safe online.
- 13.8. **Staff** are also encouraged to review their privacy settings to make sure that their profiles and photographs are not viewable by the general public.
- 13.9. Although these networks are used by staff in their own time, staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks.
- 13.10. It is recognised that some such services may have an appropriate application in school, however, where such activities are planned, a separate account should be set up for the purpose and there should be no connection made between personal and school accounts used for educational purposes. Any such accounts and activities should be approved by a member of the SMT prior to use.
- 13.11. It is never acceptable to accept a friendship request from a child from the school, as in almost all cases children of primary age using such networks will be breaching the terms and conditions of use of those networks.
- 13.12. It is also extremely inadvisable to accept as friends, ex-pupils who are still minors.



## 14. Managing Filtering

**14.1.** At present, Runnymede St Edward's School uses 'Content Keeper', a dynamic service which filters Internet sites and we also endeavour to block unsuitable sites as reported.

**14.2.** Our email facility is also filtered to prevent malicious damage and SPAM.

**14.3.** To this end we will:

- Work with our Internet Service Provider (BT) to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL must be reported immediately to the e-Safety Coordinator.
- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

## 15. Mobile Phones and Hand-held Devices.

**15.1.** In line with our Social Media policy, Mobile phones should not be used in school time by any adults or children. Choristers are required to surrender their mobile phones for security during the school day.

**15.2.** It is not acceptable to have them on view in the classroom and responding to calls/messaging there is forbidden. The sending of abusive or inappropriate text messages is strictly forbidden and will result in disciplinary action.

**15.3.** We have signs to show that mobiles are not to be used in school.

## 16. Other Portable Equipment

**16.1.** The school provides portable Computing and ICT equipment such as laptop computers, colour printers, Learnpads (tablet computers) and digital cameras to enhance the children's education and to allow staff to make efficient use of such equipment to enhance their own professional activities.

**16.2.** Exactly the same principles of acceptable use apply as in other sections of this policy.

- Equipment may be in the care of a specific individual, but it is expected that all staff may wish to benefit from the use of a laptop computer and access should be negotiated with the individual concerned. Any difficulties should be referred to the Computing and ICT co-ordinator;
- Certain equipment will remain in the care of the Computing and ICT co-ordinator, and may be booked out for use according to staff requirements. Once equipment has been used, it should be returned to the resource area (Computing and ICT room);
- Equipment such as laptop computers can be taken offsite for use by staff in accordance with the E-Safety Policy and the equipment is fully insured from the moment it leaves the school premises. The cover excludes theft or attempted theft from an unattended vehicle unless the vehicle is locked, there are signs of forced entry and the property is out of sight in a locked compartment or boot within the vehicle.
- Any costs generated by the user at home, such as phone bills, printer cartridge etc. are the responsibility of the user;
- Where a member of staff is likely to be away from school through illness, professional development (such as secondment etc.) or maternity leave, arrangements must be made for any portable equipment in their care to be returned to school. In the event of illness, it is up to the school to collect the equipment if the individual is unable to return it;
- If an individual leaves the employment of the school, any equipment must be returned;





- The use of USB pens, re-writeable CDs, etc. must be regulated. Where information has been downloaded from the internet, or copied from another computer, wherever possible, it must be emailed to school to ensure that it undergoes anti-virus scanning. If this proves to be impossible, (due to file size, technical difficulty etc.) expressed permission must be sought from the Computing and ICT co-ordinator prior to the data being transferred;
- No other software, whether licensed or not, may be installed on laptops in the care of teachers as the school does not own or control the licences for such software;

## **17. Responding to an incident of concern**

**17.1.** The e-Safety Co-ordinator (Mr Slater) acts as first point of contact for any complaint.

**17.2.** Complaints of Internet misuse will then be dealt with by a member of the Senior Management team and the Head teacher will be informed.

**17.3.** In the event of children being unintentionally exposed to undesirable materials the following steps will be taken:

- Pupils should notify a teacher immediately
- The e-Safety Co-ordinator (Mr Osborne) should be notified and the incident reported to the Headteacher.
- The incident should be recorded in a central log by which the school may reliably report the frequency and nature of incidents to any appropriate party.
- The child's parents and/or the School Governors should be notified at the discretion of the Headteacher according to the degree of seriousness of the incident.

**17.4.** Children must never intentionally seek offensive material on the Internet. Any transgression should be reported and recorded as outlined above. Any incident will be treated as a disciplinary matter and the parents of the children or children will normally be informed. If deliberate access to undesirable materials is found to be repeated, flagrant or habitual, the matter will be treated as a serious disciplinary issue. The child or children's parents will be informed and the Governing body advised.

**17.5.** Staff and pupils are given information about infringements in use and possible sanctions.

**17.6.** Sanctions available include:

- interview/counselling or meeting with Headteacher/e-Safety Coordinator;
- informing parents or carers;
- removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system.
- Referral to police.

**17.7.** Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school child safeguarding procedures.

## **18. Staff**

**18.1.** All staff will be given the School e-Safety Policy and its application and importance explained.

**18.2.** Staff are required to read and sign a 'Code of Conduct' regarding Acceptable Use of the school's information system. ( See Appendix 1)

**18.3.** Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

**18.4.** The COMPUTING AND ICT Co-ordinator ( Mr Osborne), who at present manages the filtering systems, will be supervised by Headteacher and have clear procedures for reporting issues.



**18.5.** Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

**18.6.** Any complaint about staff misuse must be referred to the Headteacher.

## **19. Parents**

**19.1.** Parents' attention will be drawn to the school's e-Safety Policy in newsletters, and on the school website and in the anti-bullying policy.

**19.2.** The school organises an 'Internet Safety Week' when parents receive leaflets, and are kept informed of activities in school. They are encouraged to access Internet Safety websites for guidance.

**19.3.** When joining the school, parents are required to read and agree to the school's Statement of Acceptable Use for Computing and ICT.

**19.4.** A partnership approach with parents is to be encouraged.

**19.5.** Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents. (See list of e-safety sites above)

<http://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/>

## **20. Pupils**

**20.1.** Rules for Internet access will be posted on or near all computer systems with Internet access.

**20.2.** E-safety training will be raise the awareness and importance of safe and responsible Internet use both at school and home.

**20.3.** Pupils will be informed that Internet use will be monitored.

**20.4.** Instruction in responsible and safe use should precede Internet access.

## **21. Specific Learning Needs (SEND)**

**21.1.** Provision for children with SEND in relation to e-Safety is made after discussion between class/subject teacher, support staff and the SEND Co-ordinator.

**21.2.** Some groups of children are potentially more vulnerable and more at risk than others when using Computing and ICT. These can include children with emotional or behavioural difficulties, learning difficulties, and other complex needs, as well as those whose English is an additional language, and looked after children.

**21.3.** Children with SEND can use the internet in educational, creative, empowering and fun ways, just like their peers. They may be particularly vulnerable to e-safety risks. For example:

- Children and young people with Autism Spectrum Disorder may make literal interpretations of content, which will affect how they respond.
- Some children may not understand much of the terminology due to language delays or disorders.
- Some children with complex needs do not understand the concept of friendship, and therefore trust everyone implicitly. They do not know how to make judgments about what is safe information to share. This leads to confusion about why you should not trust others on the internet.
- There is also growing concern around cyberbullying. We need to remember that some children with SEND may be vulnerable to being bullied through the internet, or not recognise that they are being bullied.
- In addition, some children may not appreciate how their own online behaviour may be seen by someone else as bullying.



**21.4.** Where appropriate, special adaptations, such as video presentations and the use of Widgeit cards for poorer readers, of Childnet International's SMART resources can be accessed.

**21.5.** Teachers should tackle these sensitive issues sympathetically.

## **22. Equal Opportunities**

**22.1.** All teaching and non-teaching staff at Runnymede St. Edward's are responsible for ensuring that all children, irrespective of gender, ability, ethnicity and social circumstances, have access to the whole curriculum and make the greatest possible progress.

**22.2.** Equal access needs to be planned and monitored very carefully and this must be reflected in teacher's pairs and groupings.

**22.3.** General monitoring is the responsibility of the Headteacher, the SMT and the co-ordinator.

**22.4.** Where use of a school computer proves difficult for a child because of a disability, the school will provide specialist equipment and software, so that the pupil may have access. (i.e. lower case lettering on keyboards, concept keyboards, roller ball mouse, filter screens.)

**22.5.** Pupils with learning difficulties can also be given greater access to the issues of e-Safety through the use of I.C.T.

## **23. Health and Safety Issues**

**23.1.** Seating must be adjustable and support the back when using a computer. If possible, place feet flat on the floor or use a footrest and use a document holder if necessary.

**23.2.** The top of the monitor should be just below eye level.

**23.3.** Contrast and brightness may be adjusted for your individual preference.

**23.4.** Turn the monitor at an angle towards to avoid glare from windows if necessary.

**23.5.** Lights should be dimmed and blinds drawn when the lesson involves use of the whiteboard.

**23.6.** Staring at the monitor for long periods can harm your vision and cause headaches. Look into the distance periodically – at something 20 feet away if possible.

**23.7.** Children should be encouraged to stand up at regular intervals, e.g. deliver completed work. Alternatively, stretch the hands and wrists, or rotate the head.

## **24. Review**

**24.1.** The impact of the policy will be monitored regularly with a full review being carried out bi-annually.

**24.2.** The policy will also be reconsidered where particular concerns are raised or where an e-safety incident has been recorded.

**24.3.** All staff are encouraged to feedback information and ideas about the effectiveness of this policy to the co-ordinator.  
B.Slater Sep 2018



## Appendix 1

### Staff Acceptable Use Statement



# RUNNYMEDE ST EDWARD'S SCHOOL

## Staff Acceptable Use Statement for Computing and ICT

To ensure that you as members of staff are fully aware of your professional responsibilities when using information systems and when communicating with pupils, you are asked to sign this code of conduct. Members of staff should also consult the school's e-safety policy for further information and clarification.

The computer system is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The Internet facility will be available during term time only. The school reserves the right to examine or delete files where it believes unauthorised use of the information system may be taking place, or to monitor any Internet sites visited.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that Computing and ICT includes a wide range of systems, including mobile phones/tablets, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I will not access the system without the use of an authorised account and password, which should not be made available to anyone other than the authorised system manager;
- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- I will not install any software or hardware without permission.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- I will respect copyright and intellectual property rights.
- I will ensure that electronic communications with pupils including email, and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- No e-mail attachments must be opened unless you are absolutely sure they are from known associates. If you are unsure, always delete it straight away without opening it as this is the major route for computer viruses.
- Posting anonymous messages and the forwarding of chain letters is forbidden, as is the use of public chat lines.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will ensure that mobile phones are kept out of sight and silent during teaching time.
- I will report any incident of concern regarding children's safety to the e-Safety Coordinator, the School Safeguarding Officer or Headteacher.
- I understand that 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 and the Governors will be advised.

I have read, understood and accept the Staff Code of Conduct for Computing and ICT.

Signed: \_\_\_\_\_ Capitals: \_\_\_\_\_ Date: \_\_\_\_\_

Accepted for School: \_\_\_\_\_ Capitals: \_\_\_\_\_