The Bishop Wand Church of England School

E-safety Policy

<table>
<thead>
<tr>
<th>Approved date</th>
<th>February 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review date</td>
<td>February 2018</td>
</tr>
</tbody>
</table>
E-safety is part of the school’s safeguarding responsibilities.

**Using this policy**
- Our e-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors;
- the e-safety policy was revised by: Andrew Griffiths and Isabel Cockell;
- CEOPS trained personnel: Andrew Griffiths and Isabel Cockell;
- the e-Safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and hand held games consoles used on the school site;
- the e-Safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / student.

**Managing access and security**
The school will provide managed internet access to its staff and students in order to help students to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school

- the school uses Schools Broadband/Talk Straight at their Internet Service Provider. They are one of a number of providers specialising in education;
- the school will ensure that all internet access has appropriate filtering provided by Lightspeed. Lightspeed is designed for education and is one of the most commonly used filtering products in the UK. Our system is setup to provide different levels of filtering for KS3, KS4, KS5 and staff. This is regularly checked to ensure that it is working, effective and reasonable;
- our network system has the RM/Symantec anti – virus system installed on servers and all PCs;
- access to school networks will be controlled by personal passwords. Internet is not permitted from generic accounts, other than for use at open events such as open evenings. Where unnamed accounts are used, such as for controlled assessment, staff are expected to record who uses which account;
- part of the Lightspeed product allows us to monitor the use of the internet on a user and PC basis and a log of any incidents will be kept to help to identify patterns of behaviour and to inform the e-Safety policy;
- the security of school IT systems will be reviewed regularly;
- the filtering is managed by the Technical Services Manager who is aware of procedures for reporting issues;
- low level misuse can result in internet access being withdrawn from individual students and this can be imposed by the Technical Services Manager in coordination with other staff. More serious issues can be escalated to HOY/HOD, SLT or where appropriate via the School Safeguarding and Prevent procedures;
- the school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.
**Internet Use**

The school will provide an age-appropriate e-Safety curriculum that teaches students how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others’ safety.

All communication between staff and students or families will take place using school equipment and/or school accounts.

Students and staff will be advised not to give out personal details or information which may identify them or their location.

A log on e-Safety incidents will be created and kept by the Technical Services Manager. All incidents must be reported and recorded.

**E-mail**

- students and staff may only use school provided e-mail accounts on the school IT systems. Although in urgent situations access can be provided to personal accounts by the Technical Services Manager who will supervise as required;
- staff to Student e-mail communication must only take place via a school email address or from within the learning platform;
- incoming e-mail should be treated as suspicious and attachments not opened unless the author is known;
- **all users have e-mail accounts which can send and receive to/from any e-mail account. However restrictions can be made to accounts which are misused.**

**Published content e.g. school web site, school social media accounts**

The contact details will be the school address, e-mail and telephone number. Staff or students’ personal information will not be published.

**Publishing students’ images**

The School maintains a log of parents who have not provided permission for photographs to be published online. Generally, names are not published with any photograph, however in special circumstances where it may be appropriate to publish a name, permission must be obtained from parents and the student prior to doing so.

**Use of social media including the school learning platform**

- the school will control access to social networking sites; as part of e-Safety lessons students are taught about the safe use of social media; All social media sites are blocked for all users, with the exception of a few staff who have access to Twitter to access school accounts;
- use of video social media services are blocked for most users. Occasional use of Skype is made by senior staff for recruitment purposes or meetings;
• staff and students should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community.

Use of personal devices
• personal equipment may be used by staff and/or students to access the school IT systems provided their use complies with the e-Safety policy and the relevant Internet and Email Policy;
• staff must not store images of students or student personal data on personal devices;
• the school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

Protecting personal data
• the school has a separate Data Handling Policy. It covers the use of biometrics in school, access to student and staff personal data on and off site, remote access to school systems.

Policy Decisions
Authorising access
• all staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, ICT technicians and governors) must read and electronically agree to the ‘Staff Code of Conduct before accessing the school IT systems;
• parents will be asked to sign and return a consent form to allow use of technology by their student.

Assessing risks
• the school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.

Handling e-safety complaints
• complaints of internet misuse will be dealt according to the school behaviour policy and the Internet, e-Safety and e-mail policy;
• complaints of a Safeguarding/child protection nature must be dealt with in accordance with school Safeguarding/child protection procedures;
• complaints of a child radicalisation nature must be dealt with in accordance with school Prevent procedures;
• students and parents will be informed of consequences and sanctions for students misusing the internet and this will be in line with the schools’ behavior policy.
Community use of the internet

- members of the community who will have unsupervised use of the School internet connection will have electronically agreed an Internet and Email Policy so it is expected that their use will be in accordance with the school e-Safety policy.

Communication of the Policy

To students

- students need to agree to comply with the student Internet and Email Policy in order to gain access to the school IT systems and to the internet;
- students will be reminded about the contents of the Internet and Email Policy as part of their e-safety education.

To staff

- all staff will be shown where to access the e-Safety policy and its importance explained;
- all staff must electronically agree to comply with the staff Code of Conduct in order to gain access to the school IT systems and to the internet;
- All staff will receive e-safety training on a regular basis.

To parents

- the school will ask all new parents and students to sign the Home School Agreement and the students to sign the Internet and email Policy when they register their child with the school;
- parents’ and carers’ attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school web site;
- parents will be offered e-safety training annually.

This policy relates to other policies:

- Behaviour and anti-bullying
- Safeguarding/child protection
- Internet and Email Policy
- Staff Code of Conduct