Kingskerswell Church of England Primary School

E-Safety Code of Practice

Reviewed and Approved by
Adopted by the Board of Governors;

Signed: Date:
Signed: Date:

Use of digital and video images:

- Staff are allowed to take electronically recorded material to support educational aims on school equipment.
- Personal equipment can be used (cameras and camcorders) but not mobile phones. These images need to be transferred from personal equipment to school equipment in school, and deleted from personal equipment.
- Staff must follow the school policies concerning the sharing, distribution and publication of these images. Do not share on a social networking site.
- Care should be taken when using electronically recorded material by ensuring that pupils and staff are appropriately dressed and are not participating in activities that may bring individuals or the school into disrepute.
- Staff must ensure pupils do not take or publish electronically recorded material without permission.
- Electronically recorded material published on the school website will be used as part of the schools good practice guidance.
- Staff will ensure that pupils' full names are not published or used on a website or blog particularly in association with photographs.
- Prior written permission must be received from parents/carers that they are happy for electronically recorded material to be published on school websites.
- If staff are aware of inappropriate digital/images being used by parents/carers or pupils they must report the incident to the E-Safety Co-ordinator (Daniel Yiend).

Data Protection Act 1998 – data handling

Staff must ensure data is collected and used are per the following;

- Fairly and lawfully processed.
- Processed for limited purposes only.
- Adequate, relevant and not excessive
- Accurate
- Kept for no longer than necessary
- Secure at all times
- Processed in connection with data subject rights

- Only transferred to others with adequate protection
- At all times personal data must be kept safe to minimise loss or misuse
- The use of personal data should be used on secure password protected computers and other devices approved by the school
- Laptops must be logged out when not in use
- The use of USB sticks or other removable media storage can be used in school for temporary storage of data. Personal data must not leave the premises on a USB stick or other removable media storage.
- To minimise risk, staff should ensure that data is transferred to and from a computer with virus protection (virus protection for school hardware is the responsibility of the ICT technician)

Communications:

- Mobile phones may be brought into school by staff and used as per the mobile phone policy agreement.
- Children in Year 5 and 6 must have permission to bring their phones into school which must be given to the class teacher and locked away
- Mobile phones should not be used in lesson times, even for taking photos or video imaging; school equipment should be used for these purposes
- Hand held PDAs or PSPs etc. should not be used during school hours without the approval of the Head Teacher of E-Safety Co-ordinator (Daniel Yiend)
- Staff are allowed at certain times (breaks) to use school equipment for private emails, internet sites (i.e. Amazon) and social networking sites. Staff may only communicate with pupils, parents and carers through their school email, school telephones or school mobile phones to ensure professional good practice
- Staff must be aware that communications are monitored on school equipment so appropriate language must be used at all times. Communications between staff, parents/carers and pupils must be in a professional tone
- Users must immediately report, in accordance with the school policy, if they receive an email or other communication that makes them feel uncomfortable, offended, threatened or bullied and must not respond to any such communication

- Personal email addresses, text messaging or public chat/social networking programmes must not be used for any school communications without approval from the Head Teacher or E-Safety Co-ordinator (Daniel Yiend)

Social Networking Sites

- Staff should ensure they understand how to use their privacy and security settings when using these sites.
- Staff should protect their own personal electronically recorded material to ensure they remain of a professional status; these can be hidden from certain groups/individuals.
- Staff should not comment or make reference about their school day to prevent unwanted comments or discussions. For example – I had a horrendous day to day with my children! Even innocent remarks can be misinterpreted.
- Staff should not make comments about pupils or have discussions with parents/carers on these sites to avoid unwanted responses.
- Staff should not publish digital/video imaging of pupils on these sites.
- Staff should not use inappropriate content or language on these sites, as parents, pupils or staff may find it offensive and unprofessional.
- Staff who have parents/carers on their social networking sites i.e.Facebook should ensure that they are put into a group (training can be given), if they don't accept your group invitation, then they must be removed.
- Staff should report misuse by parents/carers and pupils to the E-Safety Co-ordinator (Daniel Yiend).