



# **KING'S OAK PRIMARY SCHOOL**

## **ACCEPTABLE USE POLICY**

**May 2018**

**Policy prepared/reviewed by: Catherine Giles**

**Policy reviewed and approved by: Governing Body**

**Date of approval: 14<sup>th</sup> June 2018**

**Date of next review: May 2020**

**This school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment**

# **King's Oak Primary School Acceptable Use Policy**

## **This Acceptable Use Policy is intended to ensure:**

- that staff and volunteers will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.
- that school ICT systems are protected from accidental or deliberate misuse that could put the security of the systems and/or users and/or data subjects at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users.

## **Acceptable Use Policy Agreement**

I understand that I must use school ICT systems in a responsible way, particularly when processing data as detailed in the Data Protection Policy, to ensure that there is no risk to the safety and security of the ICT systems and all users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities, to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

## **For my professional and personal safety:**

- I understand that the school will monitor my use of the ICT systems, email and other digital communications and that misuse may be considered under the Disciplinary Procedure.
- I understand that the rules set out in this agreement also apply to the use of school ICT systems (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use during teaching and preparation times.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the Data Protection Officer.
- I will only delete documents, files and folders in line with the Record Retention Schedule and will notify the Data Protection Officer before destroying data which is not covered by this schedule.

## **I will be professional in my communications and actions when using school ICT systems:**

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission. I will immediately report any accidental deletion to the Data Protection Officer.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with students / pupils and parents / carers using official school systems. I am aware that all communications, electronic or otherwise, may become part of a request for information and will ensure that any such communication is professional in tone and manner. I am aware of the risks attached to using my personal email address / mobile phone / social networking sites for such communications.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

**The school and the Local Authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:**

- I will not use personal mobile devices (PDAs / laptops / mobile phones / USB devices etc.) in school for school business, or connect these to the school systems.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up and stored or deleted in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Data Protection Policy and Confidentiality Policy. I understand that, where digital personal data is transferred outside the secure local network, it must be encrypted and paper-based protected and restricted data must be held in lockable storage.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

## **Managing filtering**

- If staff or pupils discover unsuitable sites with inappropriate content (containing only adults) the URL (address) and content should be recorded. The Headteacher and Data Protection Officer should be informed immediately and given the details so that appropriate action can be taken.
- If staff or pupils discover an unsuitable site with illegal content (containing adults and children) the computer should have the electricity disconnected while connected to the site, after the URL (address) and content have been recorded, and secured. The Headteacher and Data Protection Officer should be informed immediately and given the details. The Headteacher will inform the police who will take appropriate action.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

## **When using the internet in my professional capacity or for school sanctioned personal use:**

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

## **I understand that I am responsible for my actions in and out of the school:**

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.

## **Social Networking**

### **Use of social media and the internet for work purposes**

In specific circumstances it may be appropriate for a member of staff to use social media as part of their work. This should only take place with the approval of the Headteacher. In such circumstances while contributing to the school's social media activities the same safeguards must be adhered to as would be with any other form of communication about the school in the public domain. Any communications made in a professional capacity through social media must not either knowingly or recklessly:

- place a child or young person at risk of harm;
- bring the school into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation;
- do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
  - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
  - using social media to bully another individual;
  - or posting images that are discriminatory or offensive or links to such content.

## **Inappropriate use of social media/internet**

The following list gives examples of the use of social media/internet sites that the school considers to be inappropriate:

- Publishing defamatory; discriminatory; illegal; sexual; racist or other offensive material;
- Publishing any material which is confidential or would breach copyright or data protection principles;
- Publishing anything of an abusive or harassing nature;
- Using social media/internet sites in a manner that would put staff/governors in breach of school codes of conduct or existing policies;
- Discussing matters relating to school, staff, pupils or parents/carers for which the social media is not considered to be an appropriate forum;
- Inappropriately holding yourself out as, or implying that you are, a representative of the school when using social media/internet sites in a private context;
- Interacting with pupils via social media/internet sites;
- Interacting with parents/carers of pupils via social media/internet sites;
- Interacting with any ex-student who is under the age of 18;
- Actively providing false or misleading information about the school, its staff or pupils;
- Online bullying;
- Inappropriately referencing other staff members, governors, students, parents or school activities/events;
- Using social media/internet sites to raise complaints/grievances – any issues should be raised via the appropriate channels (e.g. school complaints procedure).

The above is a non-exhaustive list. It is intended to provide some examples of what the school considers to be inappropriate. Each matter will be dealt with based on its own facts. School policies will be followed where relevant. The school will contact the Police where it is necessary to do so.

## **Social media in your personal life**

- The school recognises that many people make use of social media in a personal capacity. While they are not acting on behalf of the school, staff must be aware of the potential damage that could be caused to the school if they are recognised as being a member of staff.
- Staff may say that they work for a school but their online profile must not contain the school's name.
- If staff do discuss their work on social media (for example, giving opinions on their specialism or the sector in which the school operates), where appropriate they should include on their profile a statement along the following lines: "The views I express here are mine alone and do not necessarily reflect the views of the school."
- Any communications that staff make in a personal capacity through social media must not bring the school into disrepute.

## **Safeguarding and child protection guidance**

If the a member of staff receives a disclosure that a member of the school's staff is using a social

networking/internet site in a way that may put a child at risk, this should be recorded in-line with the school's Safeguarding and Child Protection Policy and Whistleblowing Policy as an allegation.

### **Staff/governors interacting with each other online**

- Governors are advised not to be "friends" with members of staff online. Reasons for this include:
  - Potential for a conflict of interest where a governor is on a selection panel/disciplinary panel where a "friend" is involved;
  - Due to the role of the Governing Body and its general responsibility for the conduct of the school, it is sensible to maintain a certain level of separation between governors and staff.
- Teachers and other staff members should also exercise caution when considering inviting work colleagues to be 'friends' on social networking sites, as this may create a conflict/difficult situation in the future.

### **Arrangements for Monitoring and Evaluation**

This policy will be monitored through half termly reports by the Data Protection Officer.

### **Review:**

This policy will be reviewed at least every two years, or as necessary, by the Data Protection Officer.