

Ridgeway Infant School is a safe happy, place where everyone does their best!

ICT ACCEPTABLE USE POLICY



Date agreed: 28TH NOVEMBER 2017

Minute Ref: FGB 17/037

Signature of Chair of FGB:

Review Due: AUTUMN 2019

Responsibility of the Full Governing Body

ICT Acceptable Use Policy

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

- ✓ 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 ICT includes a wide range of systems, including mobile phones, PDAs (Personal Digital Assistant), digital cameras, email, social networking and that this policy may also apply to personal ICT devices when used in school or for school business.
- ✓ I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- ✓ I understand that my use of school information systems, internet and email may be monitored and recorded to ensure policy compliance.
- ✓ I understand that school ICT systems, internet and email are provided to enable me to do my job and that any personal use must not impede that purpose. Personal use of any device provided by school will always be appropriate to my professional standing and will not jeopardise the reputation of the school.
- ✓ I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- ✓ I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
- ✓ I will not introduce devices (memory sticks etc.) into the system without first having checked for viruses.
- ✓ I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- ✓ I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, USB Flash Drives, digital cameras, mobile phones), unless they are secured and encrypted.
- ✓ I will not use personally owned cameras (including those on devices such as mobile phones, pocket computers or similar) to take photos of pupils within the school context.
- ✓ I will not use school cameras to take photos or videos for personal use.

- ✓ I will respect copyright and intellectual property rights.
- ✓ I will report any incidents of concern regarding children's safety to the E-Safety Coordinator, the Designated Child Protection Coordinator or Headteacher.
- ✓ I will ensure that electronic communications with pupils and parents including email, IM (Instant Messaging) and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted as inappropriate or libellous.
- ✓ My electronic communications regarding school business with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number.
- ✓ I will not have inappropriate contact with current pupils, ex-pupils or other children or young people up to the age of 19 years, where the relationship has developed as part of my 'professional' role.
- ✓ 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.
- ✓ I will ensure that I am aware of my responsibilities under **The Obscene Publications Act 1959 and 1964** and **The Children's Act 2004**.

The school may exercise its right to monitor the use of the school's information systems and internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept this code of conduct.

Name: Signed:

Date: