Internet and Online Safety User Policy

Internet Websites
- Access will be granted for all but must be age appropriate and used for educational purposes.
- Access will be filtered and monitored.
- Pupils, staff and parents informed of Internet monitoring.
- Rules for appropriate internet use will be posted near all computers.
- All pupils and staff sign an internet acceptable use policy annually.

School Website
- Home/personal info will not be published and pupil photos will not enable identification. Only pupil's first names used
- Pupil content requires parental permission and will be removed at parent's request.
- Copyright must be respected
- Website complies with publishing guidelines

Email
- Access granted for all but must be used for educational purposes.
- Pupils and staff sign an e-mail acceptable use policy annually.
- Only approved e-mail to be used.
- Pupils will not give e-mail to outside agencies/persons without permission
- Accounts updated/tracked.
- Pupils report inappropriate e-mail to CT
- Pupils must not reveal details of themselves or others or arrange meetings
- Staff report inappropriate e-mail
- External e-mail accounts are blocked
- External e-mail should be written carefully and authorised in the same way as a letter written on school headed paper
- The forwarding of chain letters is not permitted.

Complaints/Sanctions
- Staff to report any online safety concern following procedures set out in 'what to do if …' document.
- Staff misuse must be reported to the HT
- Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school safeguarding procedures. Concerns over radicalisation/ extremism are dealt with in accordance to our Safeguarding and Extremism and Radicalisation policies.
- Serious issues involve police contact
- The school will work in partnership to resolve issues
- Sanctions include: interview by HT; inform parents/carers; removal of access

Safety/Risk Management
- All reasonable precautions will be taken and risks reviewed regularly.
- Assessment of risk and educational benefit prior to pupil access.
- Partnership approach to ensure pupil protection is reviewed and improved.
- Virus protection installed and updated.
- Secure filters are installed which prevent children and adults from accessing and/ or sharing any extremist online materials.
- School/ISP cannot guarantee content.
- Clear procedures in place should inappropriate website content/ emails occur. Reported to ISP.
- Procedures set out in 'What to do if …' document shared annually with staff and displayed in staffroom.

Teaching and Learning
- Clear, progressive online safety program forms part of the Computing curriculum. Skills and behaviours embedded in other appropriate curriculum areas (e.g. PSHE).
- Pupils taught
  - Critical awareness of material
  - Effective Internet research
  - Copyright respect
- Instruction must proceed access. Plans for internet use are age appropriate with clear objectives.

Staff
- Are provided with appropriate training.
- Sign acceptable use policy annually to accept terms of responsible internet use, which are displayed in the staffroom.
- Take responsibility for the safeguarding of pupils and follow appropriate procedures to report concerns. All are vigilant of radicalisation and extremism and equipped follow correct procedures if a concern arises.
- Are informed of internet monitoring.
- Professional conduct is expected. This includes the use of social media outside of school.

Parents
- A partnership approach is adopted including demos, practical sessions and suggestions for safe Internet use at home.
- Parents provide consent for pupils to use the Internet, as well as other technologies, as part of the acceptable use agreement form at time of their child's entry to the school (including use of photographs).
- Are informed of what constitutes misuse and what sanctions may result from this.