THE COTSWOLD SCHOOL POLICY DOCUMENT

Policy:	**Staff ICT Acceptable Use Policy Agreement**
Policy Ref:	**CSP-13A ICT Use**
Version Number:	**2.0**
Date:	**September 2020**
Review Date:	**September 2021**
Authorised by:	**Awaiting Approval**
Updated by:	**Mr A Thomas Mr L Campbell**

This AUP should be read in conjunction with the school's Data Protection, E-safety and Social Media policies (these can also be found through the school's website) before being agreed to.

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

New technologies have become integral to the lives of children and young people in today's society, both within schools/academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

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 communications technologies for educational, personal and recreational use.
- school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- staff are protected from potential risk in their use of technology in their everyday work.

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

I will be professional in my communications and actions when using systems:

- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (a strong password has numbers, letters and symbols, with 8 or more

characters (newer guidance allows for three random words, not connected to yourself (not your partner's name, area you live etc. for example) to be combined to help with this) and, is only to be used on the school systems). Please talk to the IT Support team if further clarification is required.

- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, video files, documents or financial information.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act (DPA) 2018/GDPR. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.
- 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, digital cameras, mobile phones), unless they are secured (kept on your person) and encrypted (device encryption enabled) school devices are encrypted by default. Where possible I will use OneDrive / School Portal to store or upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.
- 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
- My electronic communications 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. Any pre-existing relationships which may compromise this MUST be discussed with the Senior Leadership team.
- 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 use social networking sites in school in accordance with the school's policies
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities
- If I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using the school's equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use.
- The Anti-virus/Anti-Malware/Endpoint Security provided should update automatically, both in school and at home and must be connected to a web enabled connection (at least weekly) to allow updates to be installed -
- 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 will not use personal email addresses to communicate with pupils and, where possible, refrain from using personal email in school entirely.

- 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 programs)
- I will ensure that any data stored on a portable device (e.g. laptop or a tablet) is regularly backed up
- I will not attempt to bypass any filtering and/or security systems put in place by the school (covering both laptops and computers). This is both for computers and laptops; if I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT department as soon as possible.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist 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 websites or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will report all incidents of concern regarding children's online safety to the Safeguarding team (safeguarding@thecotswoldschool.co.uk) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the ICT department as soon as possible.
- I will not try (unless I have permission) to make large 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 programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings, unless permission is gained first
- 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 Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage
- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school/academy policy to disclose such information to an appropriate authority
- I will immediately report any damage or faults involving equipment or software, however this may have happened
- I will ensure that I have permission to use the original work of others in my own work
- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.
- I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the e-Safety Coordinator or the Principal.
- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

- I understand that this acceptable use policy applies not only to my work and use of school/academy digital technology equipment in school, but also applies to my use of school/academy 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/academy
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation(s).

Further Information

- "Supporting School Staff" is an essential document to help staff understand how to protect themselves online created by Childnet International and DfE:
  http://www.digizen.org/resources/school-staff.aspx

- Teach Today is a useful website which provides useful advice and guidance for staff from industry:
  https://www.teachtoday.de/en/

- The UK Safer Internet Centre's Professional Online Safety Helpline offers advice and guidance around e-Safety for professionals who work with children and young people in the UK. The helpline provides support with all aspects of digital and online issues such as social networking sites, cyber-bullying, sexting, online gaming and child protection online. Staff can contact the helpline via 0844 381 4772, helpline@saferinternet.org.uk or can visit https://www.saferinternet.org.uk/our-helplines for more information.

- 360 Degree Safe tool is an online audit tool for schools to review current practice:
  https://360safe.org.uk/

- Children England has lots of useful guidance for people working with children and young people and, the use of technology
  https://www.childrenengland.org.uk

_____ (*12/10/2020*)
ratified by Governors and
signed as such by The Chair of Governors

This policy is written and administered with due regard to our duty and commitment as a school: to consider all aspects of equality and diversity.

THE COTSWOLD SCHOOL POLICY DOCUMENT

Policy:	**Staff ICT Acceptable Use Policy Agreement**
Policy Ref:	**CSP-13 Appendix 3**
Version Number:	**2.0**
Date:	**September 2020**
Review Date:	**September 2021**
Authorised by:	**Awaiting Approval**
Updated by:	**Mr A Thomas**

PLEASE SIGN BELOW AND RETURN THIS PAGE AS AN ACCEPTANCE OF THE ABOVE NAMED POLICY

I have read and understood the Staff ICT Acceptable Use Policy. I also agree to comply with the Staff ICT Acceptable Use Policy.

Signed: _____ Print Name: _____ Date: _____ / _____ / _____

Position: _____