St. Godric's RC Primary
Acceptable Use Policy –Adults

We love, value and respect each other.

'The best interests of the child must be a top priority in all things that affect them'.
Article 3 of the United Nations Convention on the Rights of the Child.

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.

Colleagues must ensure that they fully understand that the consequences of inappropriate activity can be severe, leading to dismissal and criminal proceedings.

1) I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, tablets, digital cameras, email and social media sites**.**

2) School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3) Staff mobile phones are allowed in school, but should only be used for communication when not working with children. Staff mobile phones should not be used during lessons or when children are present.

4) Cameras on personal phones or tablets will not be used to take pictures of children in any circumstances.

5) I understand that any hardware and software provided by my school for staff use can only be used by members of staff.

6) Personal use of school ICT systems and connectivity is only permitted with the consent of the headteacher, outside of the school day.

7) 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.

8) I will respect system security and I will not disclose any password or security information. Log in passwords should be changed on a regular basis to improve security and prevent inappropriate use of school systems.

9) It is not permitted to use another person's log in details. On occasions when log ins are shared the details of this will be recorded in an e safety log or similar document.

10) I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager. No device will be introduced to IT systems without ensuring it is free from malware, inappropriate/illegal content

11) I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. 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. All photographs and videos of children should therefore be stored on the school staff shared area. Any personal data which is being removed from the school site should be stored securely and used appropriately. Encrypted memory sticks will be used at all times especially when any pupil information (reports, assessment data, personal data, photographs etc.) is taken off site. Unencrypted memory sticks should not be used on school computing devices.

12) I will not keep professional documents which contain school-related personal information (including images, files, videos etc.) on any personally owned devices (such as laptops, digital cameras, mobile phones)

13) If I choose to use a portable device (Phone, Tablet etc…) to collect my work e-mail I will ensure that the device is locked by a pin code or password and will be wiped when I dispose of the device.

14) Digital Images or videos of pupils will only be taken from the school premises using encrypted memory sticks.

15) I will not use unapproved cloud storage systems (Dropbox, icloud etc) for storing personal data of staff or pupils.

16) I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

17) I will respect copyright and intellectual property rights. Where work is copyrighted (Including music, videos and images) I will not either download or share with others.

18) I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media.

19) I will not communicate with pupils or ex-pupils under the age of 18 using social media without the express permission of the Headteacher

20) 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 will be discussed with the Senior Leadership team. *This would include any relatives of current pupils that are my "friends" on a social media site.*

21) 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.

22) 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. This would include any comment made, even in the belief that it is private on social media.

23) I will report all incidents of concern regarding children's online safety to the Designated Child Protection Coordinator (Catherine Craig) and/or the e-Safety Coordinator (Catherine Craig) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to (Catherine Craig) the e-Safety Coordinator or (Catherine Craig) the designated lead for filtering as soon as possible.

24) I will not attempt to bypass any filtering and/or security systems put in place by the school. 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 Support Provider/Team (Michael Troman) as soon as possible

25) 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.

26) 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 (Leanne Pearson) or the Head Teacher.

27) I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of ~~i~~nformation 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.

Signed…… Date…….