George Carey Church of England Primary School

E-Safety/Use of ICT Policy

To be considered in conjunction with our **anti-bullying** policy , **equalities** policy, **behaviour** policy, **data protection** policy, **staff handbook**, and **safeguarding** policy.

Agreed by Chair of Governors September 2017

THE INTERNET

George Carey Church of England Primary School has a duty to provide pupils with quality internet access as part of their learning experience. Pupils will be taught what internet use is acceptable and what is not and given clear objectives for its use. All staff involved with teaching and learning will prepare pupils to benefit safely from the opportunities presented and ensure that they have a growing understanding of how to manage the risks involved in online activity by:

- Discussing, reminding or raising relevant e-safety messages with pupils routinely,
- wherever suitable opportunities arise
- Reminding pupils, colleagues and parents/carers about their responsibilities, which
- have been agreed through the Pupil User Agreement **(Appendix 1)** that all pupils have signed
  Have been agreed through the Parent/Carer User agreement **(Appendix 2)** that all parent/carers have signed
- Staff will guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity. Access levels will also be reviewed to reflect curriculum requirements
- Teaching pupils as a planned element of personal, social, health, economic and
- citizenship education about e-safety, cyber-bulling, misuse of technology, the law in this area and how to correctly use modern technology for positive reasons

MANAGING AND SAFEGUARDING COMPUTER SYSTEMS

The schools commission IT consultants whose responsibilities include ensuring the personal safety of staff and pupils in terms of our IT provision. It is also the IT consultants' role to work with the leadership team to ensure that the security of the schools' systems and its users are reviewed regularly. To support the maintenance of the schools' IT system:

- Workstations are secured against user mistakes and deliberate actions
- Our servers are located securely and physical access is restricted to appropriate staff
- The server operating system is secured and kept up to date
- A firewall is maintained and virus and malware protection for the whole network is installed and current
- Virus protection is installed and current on all laptops used for school activity Access by wireless devices is proactively managed (pupils cannot access the school's wireless network unsupervised) Portable media may not be used without specific permission followed by a virus check
- Unapproved software is not allowed on any school machines
- Files held on the schools' network are regularly checked
- IT consultants will review system capacity regularly
- Any administrator or master passwords for school IT systems are kept secure and available to at least two members of staff, e.g. Headteacher and the e-safety lead.
- The password is changed termly to maintain a high level of security.
- No-one except the IT consultants, Headteacher or e-safety lead is allowed to download and install software onto the network
- New users can only be given access by the IT consultants, once permission is given by a member of the Senior leadership team
- Any laptops or school technology taken off school sites must be used in accordance with this and all other relevant school policies and any damage or loss is at the expense of the staff member

MONITORING AND FILTERING INTERNET ACCESS

Internet usage at our George Carey is filtered and monitored by a system called RM Safety Net This allows members of the leadership team and governors to check internet usage, both staff and pupil. Heads of School and the SLT receive monthly summaries of activity from RM Safety Net. The LGFL and RM servers provide our internet filtering but the advantage we have is that any potential or inappropriate material can be blocked onsite at George Carey and are able to filter the information in order to highlight potentially concerning activity and identify the user involved. The advanced filtering and monitoring made available to us by **RM Saftey Net** goes above and beyond that which is mandated in Keeping Children Safe In Education (Sept. 2016).

The wireless network is secure and is password-protected, which prevents unauthorised access. Users at George Carey will be required to enter their username

and password before being able to access the network from any device. Staff have access to administer/download to PCs and laptops that are part of our domain and they have a higher privilege than pupils . All staff will follow the Acceptable Use policy **(AUP Appendix 3)**

A firewall is provided by the LGFL and RM and with RM Safety Net as an additional tool for safeguarding the school network which provides web/content filtering, ensuring that reasonable precautions are taken to prevent access to inappropriate material. However, it is not always possible to guarantee that access to unsuitable material will never occur, but the school is alerted to any material by vigilante staff and pupils. Pupils are encouraged to be vigilant and learn to become self-protective; pupils are also encouraged to report anything that is unsuitable to a member of staff.

The school cannot be responsible for eliminating everything that can be accessed through the internet.

Teachers are encouraged to inspect websites they wish to use beforehand and will be responsible for all pupils who access the internet in their lessons. The school filtering system is very dependable and blocks almost every aspect of inappropriate material. There is always potentially some risk, and this has been found mostly through websites such as You Tube, this however is a very difficult website to filter and if anything is ever found that is unsuitable then we can alert the LGFL/RM and also send a complaint to Youtube themselves, stating that we would like this material blocked. The school also has in place an alternative to YouTube for the Teachers to use and this is called TeacherTube, this is a fully educational website that filters material solely for school requirements.

https://www.teachertube.com/

All users are informed of what to do if any unsuitable material can be accessed from any computer, users will inform a member of staff and appropriate action will be taken by the designated network Technician following E- Safety procedures.

In addition to the RM Safety Net the school use monitoring software called K9 Tutor and this can access any workstation remotely on the network and any user logged onto to the network. The software can also filter bad language and any websites that are not acceptable for using on the network.

There is full back up and recovery procedures in place for school data (all child and staff data is kept securely daily onto back-up tapes on the server, using the Back Up Exec Symantec software.

NETWORK ACCESS

There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary login.

- All users are provided with a log-in appropriate to their role within the school
- Pupils are taught about safe practice with regard to login and password information
- All passwords are changed termly to maintain a high level of security
- Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information
- Remote access to school systems is limited and covered by specific agreements and is never allowed to unauthorised third party users
- Guests are not given the Wi-Fi password unless a guest login is available.

EMAIL

Email is regarded as an essential means of communication and all employees are provided with an e-mail account. Communication by email from teaching staff and administration staff to parents/carers and to external organisations should be related to school matters only. Email messages related to school matters should reflect a suitable tone and content, ensuring that the good name of the schools is maintained.

The same procedures are expected of all other employees who send emails to external organisations and colleagues.

Use of the schools' e-mail system is monitored and checked and staff should not use personal email accounts during school hours or for professional purposes. Staff are not permitted to use school email accounts to communicate with pupils at any time. See our data protection policy for further information on use of email and storing documents

PUBLISHING MATERIAL ONLINE

www.georgecareyprimaryschool.com

George Carey C of E School maintains editorial responsibility for website content to ensure that the content is accurate and the quality of presentation is maintained. The school maintains the integrity of their website by ensuring that responsibility for uploading material is always moderated and that passwords are protected.
The identities of pupils are protected at all times. Photographs of identifiable individual pupils are not published on the website unless parents/carers have provided written permission for the school to use pupils' photographs. Photographs never have names attached

Other online communication platforms

Staff and pupils are encouraged to adopt similar safe and responsible behaviour in their personal use of blogs , social networking sites and other online publishing inside and outside of school hours. Material published by pupils and staff in a social context which is considered to bring the schools' reputation into disrepute or considered harmful to, or harassment of, another child or member of the organisation will be considered a breach of conduct and behaviour and treated accordingly, as per **behaviour**, **equality**, **antibullying** and/or **staff conduct** policies/procedures.

USING IMAGES, VIDEO AND SOUND

George Carey School recognises that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are encouraged and taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.
All parents/carers are asked to sign an agreement about taking and publishing photographs and video of their pupils when offered a school or activity placement and this list is checked whenever an activity is being photographed or filmed.
For their own protection staff or other visitors to our premises are discouraged from using a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils or visitors

MOBILE PHONES

Pupils are discouraged from bringing mobile phones into school but if they do they must hand them to the school office or class teacher for safe keeping until the end of the school day. School staff are not to use mobile phones during the school day, with the exception of calling the school or the emergency services if an emergency situation arises whilst off-site (eg. school trips)

Staff are not encouraged or expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a child or parent/carer. Unauthorised or covert use of a mobile phone or other electronic device, to record voice, pictures or video is strictly prohibited.

The sending or forwarding of text messages deliberately targeting a person with the intention of causing them distress, 'cyber-bullying', will be considered a disciplinary matter for pupils and staff alike. The same is the case for other inappropriate use of mobile technology, such as 'sexting'. Pupils are taught about misuse of technology

as a matter of course through the school's personal, social, health, economic and citizenship education programme.

NEW TECHNOLOGY

The school will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an e-safety point of view. We will regularly review this policy to reflect any new technology that we use, or to reflect the use of new technology by pupils.
Employees, visitors or pupils using a technology not specifically mentioned in this policy will be expected to behave with similar standards of behaviour to those outlined in this document.

DATA (SEE OUR DATA PROTECTION & CONFIDENTIALITY POLICY)

The schools recognise their obligation to safeguard staff and pupils' personal data including that which is stored and transmitted electronically. We ensure:

- Pupils are taught about the need to protect their own personal data as part of their safety awareness and the risks resulting from giving this away to third parties
- Staff are provided with appropriate levels of access to the schools' management information systems (Integris) which holds child data.
- Passwords are not shared and administrator passwords are restricted and kept securely
- Staff are aware of their obligation to keep sensitive data secure when working on computers outside of school
- When we dispose of old computers and other equipment we take due regard for destroying information which may be held on them
- Remote access to computers is restricted to authorised staff and teachers & leaders
- There is full back up and recovery procedures in place for school data (all child and staff data is kept securely daily onto backup tapes on the server, using the Back Up Exec Symantec software
- Where sensitive staff or child data is shared with other people who have a right to see the information, for example professionals in social care teams, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any spare copies
- All staff sign a contract which includes a confidentiality section when commencing work at George Carey C of E Primary School
- Please refer to our **data protection** policy.

E-SAFETY INCIDENTS

Any incidents where pupils do not follow the User Agreement will be dealt with following the school's **behaviour policy** and procedures.

In situations where a member of staff is made aware of a serious e-safety incident, concerning pupils, visitors or staff, they will inform the Headteacher or the Designated Safeguarding Lead or Deputy or a member of the Senior leadership Team who will respond in the most appropriate manner, according to the flowchart (**Appendix 4.)**

Instances of cyber-bullying will be taken very seriously and will be dealt with using the schools' **anti-bullying procedures** and the organisation's disciplinary procedures. The organisation recognises that staff as well as pupils may be victims and will take appropriate action in either situation.

Incidents that create a risk to the security of the schools' network, or create an information security risk to the organisation, will be referred to the Headteacher Appropriate advice will be sought and action taken to minimise any risks and prevent further instances occurring, including reviewing any policies, procedures or guidance.

If the action breaches school policy, appropriate sanctions will be applied. The schools will decide if parents/carers need to be informed if there is a risk that child data has been lost.

George Carey C of E School reserves the right to monitor their premises' equipment and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

POLICY CYCLE REVIEW

This policy and all policies will be reviewed and updated as necessary by the Senior Leadership Team .

Dated 5 September 2017

Signed……

Robert Hoggett Chair of Governors