Churchill Gardens Primary Academy Online Safety Policy

Approved spring term 2021

Introduction

Computing in the 21st century is seen as an essential resource to support learning and teaching, alongside playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to equip our young people with the skills to access life-long learning and employment. Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning.

It is also important to recognise the constant and fast-paced evolution of computing within our society as a whole. Currently, the internet technologies children and young people have access to include:

- Websites
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting (Audio Sharing)
- Video Sharing
- Music Sharing
- Online and downloaded gaming
- Mobile/smart phones with functionality including: texting and instant messaging, video, web, audio, music, global positioning (GPS)
- Other mobile devices with similar functionality (such as tablets, laptops and gaming devices)

Whilst computing has exciting potential both within and beyond the context of education, technology has its risks. Web-based resources in particular are not moderated or policed consistently. All users need to be aware of the range of risks associated with the use of these internet technologies.

Ensuring children and young people are aware of the risks associated with the use of technologies, and helping them to adopt safer online behaviours, is vital in safeguarding them against dangers such as cyberbullying and grooming.

At Churchill Gardens Primary Academy, we do not explicitly teach computing as a discrete academic subject. Nevertheless, we are keenly aware of and understand our vital responsibility to educate our pupils on Online Safety issues. These responsibilities include teaching children the appropriate behaviours and critical-thinking skills to enable them to remain both safe and legal when using the internet and related technologies, within and beyond the context of the classroom.

This policy relates to both the fixed and mobile internet technologies provided by the school, and to any personal mobile technologies – whether these are owned by pupils, parents and staff – that are brought onto school premises.

Roles and responsibilities

Online Safety is an important aspect of strategic leadership within the school and, as such, the executive principal, principal and school governors have overall responsibility to ensure that this policy and practices are embedded and monitored. The named Online Safety coordinators in our school are Shahid Sahil and Liane Tylee (who have been designated this role). They report to Tamara Spring, the Designated Safeguarding Lead. It is the role of the coordinator to keep abreast of current issues and guidance in association with organisations such as Westminster LA, CEOP (Child Exploitation and Online Protection), UKCCIS, and Childnet.

The school's senior management and governors are updated by the principal and coordinators, and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy — supported by the school's Acceptable Use Policy and Agreement for staff, governors, and visitors (see appendix) — is designed to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: the Child Protection Policy; the Health & Safety policy; and the Behaviour Policy (including the Anti-Bullying Policy). It also relates to the PSHE and RSE curriculums.

Skills development for staff

The following procedures are in place to ensure that school staff are kept up-to-date with Online Safety at the school:

- All staff receive regular information and training on Online Safety issues in the form of updated Acceptable Use Agreements.
- New staff receive information on the school's Acceptable Use Policy as part of their induction.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the online context. They are aware of what they should do in the event of misuse of technology by any member of the school community.
- All staff are expected to incorporate Online Safety awareness within the PSHE and RSE curriculum areas.

Managing the school Online Safety messages

We endeavour to embed Online Safety messages across the curriculum wherever the internet and/or related technologies are used. Online Safety is particularly reinforced during PSHE and RSE lessons in relation to cyberbullying and grooming.

Computing in the curriculum

Computing is not currently taught as an explicit curriculum subject at Churchill Gardens Primary Academy.

Password security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords, and these passwords are not shared with anyone else.

- All users must read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's policy.
- Users will be provided with an individual network username.
- Staff must be aware of their individual responsibilities to protect the security and confidentiality of school networks and management information systems, including ensuring that passwords are not shared and that these passwords are changed periodically.
- Individual staff users make sure that workstations are not left logged in or, if necessary, are password-locked.

In our school, all staff are expected to comply with the above regulations at all times.

Data Security

The accessing and appropriate use of school data is something that our school takes very seriously.

- Staff are aware of their responsibility when accessing school data. The school principal determines the level of access available to individual staff members.
- Any data taken off the school premises must be encrypted.
- The school network is backed up internally by our trust's IT department.

Managing the Internet

The internet is an open communication medium, available to all people at all times. Anyone can view information, send messages, discuss ideas and publish material. This makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

To help protect our young people from harm on the internet, we follow the below regulations:

- Raw image searches (e.g. a Google Images search) are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested. These will have been checked by the teacher.
- It is advised that parents recheck these sites and supervise any online work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Churchill Gardens Primary Academy is aware of its responsibility when monitoring staff communication under current legislation. We take into account: the Data Protection Act 1998; the Telecommunications (Lawful Business Practice) (Interception of Communications) 7 Regulations 2000; the Regulation of Investigatory Powers Act 2000; and the Human Rights Act 1998.

Staff are aware that school-based email and internet activity can be monitored.

The school uses management control tools for controlling and monitoring workstations. If staff discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the IT department.

Pupils and staff are not permitted to download programs or files on school equipment; this is controlled by the trust's IT department.

If there are any issues related to viruses or anti-virus software, the trust's IT department should be informed via the office administrator.

Managing other communication & networking technologies

The internet includes a wide range of communication & networking tools and websites. Children need to be educated about appropriate ways of communicating, and about the risks of making personal information too readily available online.

If used responsibly (both within and beyond the educational context) communication & networking technologies can be easy-to-use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of the content, contact, culture and commercialism of some of these tools and websites. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from any communication & networking tools and websites.

At present, the school does not teach computing as part of the academic curriculum. However, we do run lessons on online safety in Safer Internet Week (which usually runs in the spring term). The guidance provided to pupils encompasses the following:

- All pupils are advised to be cautious about the information they provide to others on sites (for example, recognising that other users might not always be who they say they are).
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites. They are taught to consider the appropriateness of any images they post due to the difficulty of removing images once they are placed online.
- Pupils are reminded to avoid giving out personal details on such sites which may identify their identity or location (for example, their full name, address, mobile and home phone numbers, school details, email addresses or specific hobbies and interests).
- Pupils are advised to set and maintain profiles on the maximum privacy setting, and to deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Pupils are asked to report any incidents of online bullying to the school.

In addition, all school staff understand that it is highly inappropriate to use social networking sites and other personal communication tools with pupils and/or parents (e.g. via Facebook, Myspace, Twitter, Instagram, WhatsApp, or personal email addresses, etc.).

Mobile technologies

Many emerging technologies offer new and exciting opportunities for teaching and learning. These include a move towards personalised learning and 1:1 device ownership for children and young people.

Many existing mobile technologies (such as portable media players, gaming devices, smart phones, tablets, etc.) are already familiar to children in their lives outside of school. Allowing such personal devices to access the school network can provide immense benefits for collaboration, but can also create risks associated with misuse, inappropriate communication, etc.

Emerging technologies will be examined for their educational benefit, and all risks will be assessed, before such use of personal devices will be facilitated in school. Our school chooses to manage the use of these devices in the following ways so that users utilise them appropriately.

Personal mobile devices (including phones)

- Only under extreme circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device. If they do so, they should always dial 141 to block their number first.
- Pupils in Year 6 are allowed to bring personal mobile devices/phones to school but must hand them in at the office every morning. At all times, the device must have silent mode enabled.
- Technology may be used, for educational purposes, as mutually agreed with the principal. The device user, in this instance, must always ask the prior permission of the bill payer.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image, video or sound recordings are made on the devices of any member of the school community.
- Capturing images and/or video is not allowed by pupils/staff unless on school equipment and for educational purposes.
- Users bringing personal devices into school must ensure that there is no inappropriate or illegal content on the device.

School-provided mobile devices (including phones)

- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image, video or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies (e.g. phones, laptops, etc.) for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop or tablet for staff, only this device may be used to conduct school business outside of school.

Sexting

In January 2017, the UK Council for Child Internet Safety (UKCCIS) published a comprehensive 50-page guidance document Sexting In Schools. This document, created by expert agencies and with the backing of the Department for Education, includes everything that DSLs, principals and other senior school leaders need to deal appropriately with incidents of sexting. The guidance includes (but is not limited to) legal advice, education tools, flowcharts for responding to incidents, research and analysis tools and aids for staff training.

Managing email

The use of email within most schools is an essential means of communication for staff. In the context of a school, however, email should not be considered private.

In educational settings, email can also offer significant benefits that include direct written contact between schools on different projects (both staff-based or pupil-based, and within the UK or internationally). We recognise that pupils need to understand how to style an email in relation to their age and be aware of what constitutes good 'netiquette'. Moreover, in order to achieve Computing Level 4 or above, pupils must have experience of sending and receiving emails.

The following procedures and regulations apply to all in-school email use.

- The school gives all staff an individual Microsoft Office Outlook account to use for school business. This is to minimise the risk of receiving unsolicited or malicious emails, and to prevent personal profile information being revealed.
- It is the responsibility of each account holder to keep their email password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary, email histories can be traced. Only a staff's school email address should be used for school business.
- Under no circumstances should members of staff contact pupils or parents, or conduct any other school business, using a personal email addresses.
- The school requires a standard disclaimer to be attached to all email correspondence. This states that, "The views expressed are not necessarily those of the school". The responsibility for adding this disclaimer lies with the account holder.
- Emails sent to an external organisation should be written carefully before sending, and with the same etiquette as a letter written on school-headed paper.
- Staff who are sending emails to external organisations or parents are advised to send via their designated Microsoft Office Outlook account.
- All email users are expected to adhere to the generally accepted rules of network etiquette ('netiquette'), particularly in relation to the use of appropriate language, and with regards to not revealing any personal details about themselves or others in email communication. They should not arrange to meet anyone without specific permission.
- Staff must inform IT department if they receive an offensive email.

Safe use of images/ videos

Taking of images/ videos

Digital images/ videos are easy to capture, reproduce and publish and, therefore, can be easily misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public without first seeking the consent of any individuals involved and considering the appropriateness of the images or videos taken.

With the written consent of staff and parents (on behalf of pupils), the school permits the appropriate taking of images/ videos by staff and pupils **using school equipment**.

Staff are **not permitted** to use **personal devices**, (e.g. personal mobile phones, tablets or cameras), to record images of pupils (including when on field trips). However, with the express permission of the principal, images can be taken provided that they are transferred immediately and solely to the school's network, and then immediately deleted from the staff member's device.

The consent of adults who work at the school

- Permission to use images/videos of all staff who work at the school is sought on a regular basis and a copy of this permission is located in the personnel file.
- Parents must seek permission to take photos/ videos at school events, and must agree that they will not post these images/ videos on the internet.
- Parents are requested not to video school performances. Video of performances will be captured by school staff and will be stored safely on the school system.

Publishing pupils' images, videos and work

On a child's entry to the school, all parents/guardians will be asked whether they give permission for the school to use their child's work, photos or videos in the following ways:

- on the school website;
- in the school prospectus and other printed publications that the school may produce for promotional purposes;
- recorded and/or transmitted on a video or webcam;
- in display material that may be used in the school's communal areas;
- in display material that may be used in external areas (i.e. in an exhibition promoting the school); and
- in general media appearances (e.g. local and national media, or local and national press releases highlighting a particular school activity, either through traditional mediums or electronically).

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue (e.g. the divorce of parents, custody issues, etc.). However, parents/ carers may withdraw permission, in writing, at any time.

To protect pupils' identities, names will not be published alongside images or vice versa. The email and postal addresses of pupils will not be published. Pupils 'full names will not be published.

Before posting pupils 'work on the internet, a check needs to be made to ensure that permission has been given for work to be displayed. In addition, only the Web Manager has the authority to upload to the school's public website.

Storage of images/ videos

- Any images/ videos of children are stored on the school's network.
- Staff are not permitted to use any personal portable media (e.g. USB storage devices) for storage of images without the express permission of the principal.
- Rights of access to this material are restricted to the teaching staff, and only within the confines of the school network.
- All images/videos of pupils are deleted when pupils leave the school.

Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to the school's CCTV's systems are the principal, the DSL and the office manager. Notification of CCTV use is displayed at the front of the school.
- We do not use publicly-accessible webcams in school other than for special projects (such as nature cams) which are streamed to the web.
- Webcams in school are only ever used for specific learning purposes, (e.g. monitoring hens 'eggs)
- Images of children and adults are never broadcast.
- Misuse of a webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document).
- Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.

Cyberbullying and online relationships

The school's Relationships & Sex Education curriculum (RSE) provides a set of preventative tools which help safeguard pupils against cyberbullying and grooming. The school has a comprehensive RSE policy in place which includes the appropriate teaching & learning of:

- Private and personal spaces
- Appropriate and safe relationships versus inappropriate and harmful relationships
- Consent

Misuse and Infringements

Complaints

Any complaints relating to Online Safety should be made to directly to the principal and the IT department. Incidents should be logged and due processes should be followed.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. Any breaches must be reported immediately to the IT department.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the IT department. Depending on the seriousness of the offence, such behaviour may lead to:
    - Reports to the DSL
    - Investigation by the principal and/or LA
    - Immediate suspension
    - Dismissal
    - Involvement of the police

Equal Opportunities

Pupils with additional needs

The school endeavours to work in partnership with parents to convey a consistent message to all pupils. This in turn should aid the establishment and future development of the schools 'rules.

Staff are aware that some pupils will require additional reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safety issues.

Parental Involvement

We believe that it is essential for parents/ carers to be involved fully with promoting Online Safety (both within and outside of school), whilst simultaneously appreciating the benefits provided by technologies more generally.

We regularly consult and discuss technology use with parents/ carers, and we seek to promote a wide understanding about the link between technology and safeguarding.

Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school policy through questionnaires.

Parents/ carers are required to make a decision as to whether they consent to images of their child being taken and/or used in the public domain (e.g. on the school website).

The school disseminates information to parents, where appropriate, in the form of:

- Information and celebration evenings
- Website postings
- Newsletter items

Reviewing this Policy

Review Procedure

This policy will be reviewed regularly. All due consideration will be given to the implications for future whole-school development planning.

The policy will be amended if new technologies are adopted or the UK's central government changes the orders or guidance in any way.