# ONLINE SAFEGUARDING POLICY

# 2018

*Rodmarton Primary School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share the same commitment. All staff and volunteers are subject to an enhanced DBS check.*
*Please refer to the school's Child Protection Policy for more information*

*We have carefully considered and analysed the impact of this policy on equality and the possible implications for pupils with protected characteristics, as part of our commitment to meet the Public Sector Equality Duty requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.'*

Agreed by Governors: July 2019
Review Date: Summer Term 2021

# Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as 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 arm our young people with the skills to access life-long learning and employment. Information and Communications Technology 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 ICT within our society as a whole. Currently, the internet technologies children are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- APPs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies. At Rodmarton Primary School we understand the responsibility to educate our pupils on Online Safeguarding issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, Governors, visitors and pupils) are inclusive of fixed and mobile internet technologies provided by the school (such as PCs, laptops, webcams, whiteboards, digital video equipment, etc.). Due to the constant changes taking place within technology, this policy may not contain the most recent developments. We will, however, endeavour to add any important issues to the policy on our website.

# Roles and Responsibilities

As Online Safeguarding is an important aspect of strategic leadership within the school, the Head and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the Headteacher to keep abreast of current issues and guidance through organisations such as SWGfL, Becta, CEOP (Child Exploitation and Online Protection) and Childnet. The Governors are updated by the Headteacher 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 (signed agreements) for staff, Governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: safeguarding, child protection, health and safety and behaviour (including the anti-bullying).

### Online Safeguarding skills development for staff

Our staff receive timely information and training on Online Safeguarding issues in the form of staff meetings and notices. New staff receive information on the school's acceptable use policy as part of their induction. All staff have been made aware of individual responsibilities relating to the safeguarding of

children within the context of Online Safeguarding and know what to do in the event of misuse of technology by any member of the school community. All staff are encouraged to incorporate Online Safeguarding activities and awareness within their curriculum areas. We endeavour to embed Online Safeguarding messages across the curriculum whenever the internet and/or related technologies are used. The Online Safeguarding policy will be introduced to the pupils at the start of each school year.

**Online Safeguarding in the Curriculum**

The school provides opportunities within a range of curriculum areas to teach about Online Safeguarding.
Educating pupils on the dangers of technologies that maybe encountered outside school is done formally when opportunities arise and as part of the Online Safeguarding/Computing curriculum.
Older pupils will be made aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them. Pupils in upper Key Stage 2 are also taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.

Older pupils are made aware of the impact of online bullying and will know how to seek help if they are affected by these issues. Pupils will also be aware of where to seek advice or help if they experience problems when using the internet and related technologies eg parent/carer, teacher/ trusted staff member or an organisation such as Childline/ CEOP report abuse button.

Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.
All users, including pupils, read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's Online Safeguarding Policy. Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others. Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks.

## Infrastructure

Rodmarton Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account: Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998. Rodmarton Primary School has a monitoring solution via the South West Grid for Learning where web-based activity is monitored and recorded. School Internet access is controlled through the LA's (Local Authority) web filtering service.

Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required. The school does not allow pupils access to internet logs. If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the teacher and then to the Headteacher. It is the responsibility of the school to ensure that Anti-virus protection is installed on all school machines. This automatically updates.

Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility to install or maintain virus protection on personal systems. Pupils and staff are not permitted to download programs or files on school based technologies. If there are any issues related to viruses or anti-virus software, the Headteacher should be informed.

**Data Security**

The accessing of school data is something that the school takes very seriously. Staff are aware of their responsibility when accessing school data. They must not access data outside of school, take copies of the data, allow others to view the data and/or edit the data unless specifically requested to do so by the Headteacher and/or Governing Body.

All personal data is only accessed at school by one member of staff and unless there is an emergency this would not be accessed outside of school.

### Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the South West Grid for Learning (SWGfL) is logged and the logs can be randomly but regularly monitored. Whenever any inappropriate use is detected, it will be followed up. The school allows pupils to have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology. Staff will preview any recommended sites before use. Raw image searches are not allowed when working with pupils. If Internet research is set for homework, it is advised that parents check the sites and supervise the 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.

## Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and
Smart phones are familiar to children outside of school too. They often provide a collaborative, well known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

### Personal Mobile devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use. Separate, individual permissions may be granted for the use of a personal device for specific purposes. Such permissions must be authorised by the Headteacher and a record kept. Under certain circumstances the school allows a member of staff to contact a pupil or parent/ carer using their personal device. 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 or sound recordings are made on these devices of any member of the school community. Any images must be downloaded to the school server and deleted from personal devices. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Pupils are not permitted to bring mobile phones in to school. If they are found to have these on their person, the mobile phone will be confiscated and parents/ carers will be asked to collect the device from the head teacher.

### School provided Mobile devices (including phones)

The school has a mobile phone which staff can use when they take pupils off the school site. The sending of inappropriate text messages between any members of the school community is not allowed.

The school provides mobile technologies such as cameras and ipad minis for offsite visits and trips. Where the school provides a laptop for staff, only this device may be used to conduct school business

outside of school and should not be used by anyone other than the member of staff that the laptop is assigned to.

## Managing email

The use of email within most schools is an essential means of communication for staff. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including direct written contact between schools on different projects, be they staff based or pupil based, within school or international.

The school gives all staff and Governors (and the Clerk to the Governing Body) their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed. It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business. Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper. Staff sending emails to external organisations, parents or pupils are advised to cc. the Headteacher. All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette), particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication. Staff must inform (the Headteacher) if they receive an offensive e-mail.

## Safe Use of Images

Digital images are easy to capture, reproduce and publish and, therefore, 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 consent and considering the appropriateness.
With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils.

### Publishing pupils' images and work

On a child's entry to the school, all Parent/Carer(s) will be asked to give permission to use their child's work/photos 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/ transmitted on a video or webcam, in display material that may be used in the school's communal areas, display material that may be used in external areas (ie exhibition promoting the school), general media appearances (eg local/ national media/ press releases sent to the press highlighting an activity).
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 eg divorce of parents, custody issues. Parent/Carer(s) may withdraw permission, in writing, at any time.
Pupils' surnames will not be published alongside their image. E-mail and postal addresses of pupils will not be published.

### Storage of Images

Images/ films of children are stored on the school computers. Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher. Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.

**Webcams and CCTV**

We do not use publicly accessible webcams in school. Webcams in school would only ever be used for specific learning purposes eg monitoring hens' eggs, and never using images of children or adults. Misuse of the webcam by any member of the school community will result in sanctions.

## Misuse and Infringements

Complaints relating to Online Safeguarding should be made to the Headteacher. Incidents and infringements should be logged. Any complaints or concerns regarding the Head Teacher should be reported to the School's Chair of Governors please see Whistle Blowing Policy for more information.

**Inappropriate material**

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Headteacher/Online Safeguarding co-ordinator. Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Headteacher/Online Safeguarding co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

## Equal Opportunities

Pupils with additional needs
The school endeavours to create a consistent message with parents for all pupils and this, in turn, should aid the establishment and future development of the schools' Online Safeguarding rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safeguarding issues. Internet activities are planned and well managed for these children.

Parent/Carer(s) and pupils are actively encouraged to contribute to the school Online Safeguarding policy by letter and by reporting unsuitable sites etc. to the Headteacher/Online Safeguarding co-ordinator. Parent/Carer(s) are asked to read through and sign acceptable use agreements on behalf of their child on admission to school. Parent/Carer(s) are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (eg on the school website). The school disseminates information to parents relating to Online Safeguarding where appropriate in newsletter items.

## Writing and Reviewing this Policy

This policy will be reviewed every (24) months and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

**Acceptable Use**

aims:

- Ensure that pupils benefit from all learning opportunities offered by the Internet resources provided by the school in a safe and controlled manner.
- Ensure that all staff benefit from Internet access, with clear guidance on safe and acceptable use.
- Make staff and pupils aware that Internet use in school is a resource and a privilege. If the terms are not met that the privilege will be taken away.
- Provide guidance to staff and pupils about the acceptable use of mobile technologies, both the school's and personal items, which are brought into school.
- Clearly assert that the school and its paid providers will monitor the use of the ICT systems, email and other digital communications.

**Online Safeguarding**

Virus protection software is used and updated on a regular basis. The headteacher is responsible for the school's Online Safeguarding and will take advice from experts employed by the school to assist in this matter, currently Silverglobe.

**Pupils' Access to the Internet:**

Rodmarton School use a Gloucestershire County Council "filtered" Internet Service, which will minimise the chances of pupils encountering undesirable material. Rodmarton School will normally only allow children to use the Internet when there is a responsible adult present to supervise. However, it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen. Members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils how they may use ICT and our expectations of them. Teachers will have access to pupils' emails, where applicable, and other Internet related files and will check these on a regular basis to ensure expectations of behaviour are being met.

**Expectations of Pupils and Staff using the Internet:**

- All pupils are expected to read and agree the Internet Agreement.
- At Rodmarton, we expect all pupils and staff to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access and language they use.
- Pupils and staff using the World Wide Web are expected not to deliberately seek out offensive materials.
- Should any pupils or staff encounter any such material accidentally, they are expected to report it immediately to the Headteacher or ICT leader so that the Service Provider can block further access to the site.
- Pupils are expected not to use any rude language in their email communications and contact only people they know or those the teacher has approved. They have been taught the rules of etiquette in email and are expected to follow them.
- Pupils must ask permission before accessing the Internet and have a clear idea why they are using it.
- Pupils and Staff should not access other people's files unless permission has been given.
- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the Internet. This is to prevent corruption of data and avoid viruses.
- No programs on disc or CD Rom should be brought in by pupils from home for use in school although staff can seek permission from the Headteacher. This is for both legal and security reasons.
- Homework completed at home may be brought in on floppy disc, CD-ROM or memory stick, but this will have to be virus scanned by the class teacher before use.

- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.
- Pupils and Staff consistently choosing not to comply with these expectations will be warned and, subsequently, may be denied access to Internet resources. They will also come under the general discipline procedures of the school which comprises an escalating set of measures including a withdrawal of privileges.
- Uploading and downloading of non-approved software will not be permitted.

**School Website:**

- The website will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff.
- The publications of children's work will be decided by a teacher/Headteacher.
- Photographs and video focusing on individual children will not be published on the school website without parental permission (gained annually).
- The school website will avoid publishing the full names of individuals in a photograph. First names, and the initial of the surname when necessary, will be used.
- The school will ensure that the image files are appropriately named and will not use pupils' names in image file names if published on the web.

**Personal Devices:**

Staff and pupils may only use their own technology in school as part of a pre-arranged educational activity, with permission from the Headteacher. Inappropriate use is in direct breach of the school's Acceptable Use Policy. Pupils are not permitted to bring mobile phones in to school. Pupils are not permitted to bring mobile phones in to school. If they are found to have these on their person, the mobile phone will be confiscated and parents/ carers will be asked to collect the device from the head teacher.

**Sanctions:**

Persistent Misuse of the internet by pupils will result in reducing access to the Internet. Misuse of other technologies will result in a complete ban and/or confiscation. Both of these actions will take place for a set period of time agreed by the Headteacher. Parent/Carer(s) will always be notified.

If the school becomes aware of a pupil using facebook or an equivalent social networking site that is inappropriate for the age of the pupil, the Headteacher reserves the right to report that pupil to the networking company. Parent/Carer(s) would be informed.

**Rodmarton Primary School Pupil Internet and ICT Agreement:**

This is to be read through by pupils and parent/carer(s) and then signed. Pupils will be allowed supervised Internet Access after this is returned to school.

1. We expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access and language they use.
2. Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher.
3. Pupils are expected not to use any rude language in their email communications and contact only people they know or those the teacher has approved. It is forbidden to be involved in sending chain letters.
4. Pupils must ask permission before accessing the Internet.
5. Pupils should not access other people's files unless permission has been given.
6. Computers should only be used for schoolwork and homework unless permission has been granted otherwise.

7. No program files may be downloaded to the computer from the Internet.
8. No programs on disc or CD Rom should be brought in from home for use in school.
9. Homework completed at home may be brought in on floppy disc, CDROM or memory stick, but this will have to be virus scanned by the class teacher before use.
10. Personal printing is not allowed on our network for cost reasons (e.g. pictures of pop groups/cartoon characters).
11. No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.
12. Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to Internet resources.