Covingham Park Primary School

Online and E-Safety Policy – including Filtering and Monitoring

Date Written: April 2024

Author: Headteacher

Reviewed:

Next Review Date: April 2026

Contents

1. INTRODUCTION

At Covingham Park Primary School, we believe that IT is central to all aspects of learning, for adults and children in both the school and the wider community.

Provision should reflect the rapid developments in technology.

IT in the 21st Century is 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, we need to build in the use of these technologies in order to equip our young people with the skills to access lifelong learning and employment.

All children, whatever their needs, will have access to a range of up-to-date technologies in both the suite and classrooms. IT is a life skill and should not be taught in isolation.

This policy should be read in conjunction with the school's safeguarding policy.

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 fastpaced evolution of IT 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

• Podcasting

• Video Broadcasting

• Music Downloading

• Gaming

• Mobile/ Smart phones with text, video and/ or web functionality

• Other mobile devices such as smart watches with web functionality

All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Covingham Park Primary School, we understand the responsibility to educate our pupils on e-safety 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.

2. WHOLE SCHOOL APPROACH

All members of the school community have a responsibility for promoting and supporting safe behaviours in their classrooms and follow school e-safety procedures. The IT subject leader and SLT members will ensure they are up to date with current guidance and issues through organisations such as CEOP (Child Exploitation and Online

Protection), SWGFL advice and Child Net. They then ensure that Governors are updated as necessary.

All staff should be familiar with the school's policy including:

• safe use of e-mail

• safe use of the Internet

• safe use of the school network, equipment and data

• safe use of digital images and digital technologies, such as mobile phones and cameras

• publication of pupil information/photographs on the school website

• procedures in the event of misuse of technology by any member of the school community (see appendices)

• their role in providing e-safety education for pupils.

Staff are reminded/updated about e-safety regularly and new staff and students receive information on the school's acceptable use policy as part of their induction.

Supply Teachers must sign an acceptable use of IT agreement before using technology equipment in school (see appendix 3 for staff acceptable use agreement).

3. E-SAFETY IN THE CURRICULUM

IT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety.

• We provide opportunities within the computing and PSHE curriculum areas to teach about e-safety. https://projectevolve.co.uk/toolkit/

• Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the curriculum.

• Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling, and activities as part of the computing curriculum.

• Pupils are aware of the impact of online bullying through PSHE and computing and are taught how to seek help if these issues affect them. Pupils are also aware of

where to seek advice or help if they experience problems when using the internet and related technologies (cyber-bullying)

• Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the computing curriculum

• Pupils are taught about the risks inherent in using social media, particularly if they are contacted by people they do not know

4. MANAGING INTERNET ACCESS

Children will have supervised access to Internet Resources.

• Wherever possible, staff should preview any recommended sites before use.

Particular care must be taken when using search engines with the children as these can return undesirable links.

• Raw image searches are discouraged when working with pupils.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents need to be advised to supervise any further research.

• Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

• If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the teacher. The safeguarding team must then be informed if appropriate.

• It is the responsibility of the school, by delegation to Wave 9, to ensure that antivirus protection is installed and kept up-to-date on all school machines.

5. EMAIL

The use of email within school 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, between schools or international.

• The school gives staff 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.

• Under no circumstances should staff contact pupils or parents using personal email addresses.

• Pupils may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes.

• The forwarding of chain letters is not permitted in school.

• Pupils must immediately tell a teacher/ trusted adult if they receive an offensive email.

• All pupils must use appropriate language in e-mails and must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone.

• Staff must inform a member of SLT if they receive an offensive e-mail.

6. PUBLISHING PUPIL IMAGES AND WORK

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

• on the school web site

• 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. exhibition promoting the school

• general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically.)

• School's social media platforms

• Pupils' names will not be published alongside their image and vice versa without permission from the parents. Full names will not be published.

7. SOCIAL NETWORKING AND PERSONAL PUBLISHING

We block/filter access for pupils to social networking sites. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

• Pupils will be advised never to give out personal details of any kind that may identify them or their location.

8. MANAGING EMERGING TECHNOLOGIES

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

• Children will be strongly advised not to bring phones into school.

• Parents and children sign a consent form (Appendix 2)

• Mobile phones will not be used during lessons or formal school time.

• Smart watches will not be allowed in school for children

• All classes have access to a set of tablets and a mobile IT trolley. The trolley can be booked using the established protocol

9. DATA PROTECTION

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

• Data can only be accessed and used on school computers. Staff are aware they must not use their personal devices for accessing any children/ pupil data.

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals' rights of access to their personal data, compensation and prevention of

processing. http://www.hmso.gov.uk/acts/acts1998/19980029.htm

10. RESPONDING TO E-SAFETY INCIDENTS/COMPLAINTS

As a school, we will take all reasonable precautions to ensure e-safety. However, owing to the global scale and inter-linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access. Complaints

relating to e-safety should be made to a member of the senior leadership team. Any complaint about staff misuse must be referred to the Head teacher.

• All users are aware of the procedures for reporting accidental access to

inappropriate materials. Any breach must be immediately reported.

• Deliberate access to inappropriate materials by any user will lead to the incident being logged and, depending on the seriousness of the offence; investigation by the Head teacher/ LEA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences

• Pupils and parents will be informed of the complaint's procedure.

• Parents and pupils will need to work in partnership with staff to resolve issues.

11. CYBER BULLYING

Cyberbullying is the use of IT, particularly mobile phones and the internet, to deliberately upset someone else. The whole school community has a duty to protect all its members and provide a safe, healthy environment. The Educations and Inspections Act 2006 states that Head teachers have the power 'to such an extent as is reasonable' to regulate the conduct of pupils when they are off site.

Although bullying is not a specific criminal offence in the UK law, there are laws that can apply in terms of harassing or threatening behaviour, for example, or indeed menacing and threatening communications.

There are many types of cyber-bullying; these are listed in Appendix 3

12. PREVENTING CYBER BULLYING

It is important that we work in partnership with pupils and parents to educate them about Cyberbullying as part of our e-safety curriculum.

They should:

• understand how to use these technologies safely and know about the risks and consequences of misusing them

• know what to do if they or someone they know are being cyber bullied.

• report any problems with Cyberbullying. If they do have a problem, they can talk to the school, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP) to do something about it.

Additional online advice on how to react to Cyberbullying can be found on

www.kidscape.org and https://www.bullying.co.uk/cyberbullying/

Supporting the person being bullied

Support will be provided in some or all of the following ways:

• Give reassurance that the person has done the right thing by telling someone and inform parents.

• Make sure the person knows not to retaliate or return the message.

• Help the person keep relevant evidence for any investigation (taking screen capture shots, not deleting messages.)

• Check the person knows how to prevent it from happening again e.g. blocking contacts, changing contact details.

• Take action to contain the incident when content has been circulated: remove content, contact the host (social networking site) to get the content taken down, use disciplinary powers to confiscate phones that are being used to cyber bully –ask the pupil who they have sent messages to.

Investigating Incidents

All bullying incidents should be recorded and investigated on the safeguarding chronology. We will then investigate as fully as any other bullying incident.

13. WORKING IN PARTNERSHIP WITH PARENTS

Parents/carers are asked to read through and sign the school's Acceptable Use Policy on behalf of their child on admission to school (see appendix 1).

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

• A partnership approach with parents will be encouraged. This includes parents' evenings with suggestions for safe home Internet use.

• Advice on filtering systems and educational activities that include safe use of the Internet will be made available to parents.

14. REVIEW

There will be an on-going opportunity for staff to discuss with SLT any issue of safety that concerns them.

This policy will be reviewed every three years. However, the policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

APPENDIX 1 – PUPIL ACCEPTABLE USE POLICY

Covingham Park Primary School

Pupil's acceptable use of the school's ICT facilities and internet

Name of pupil:

When using digital devices, I will:

• only access equipment when a trusted adult has given me permission and is present

• not deliberately look for, save or send anything that could make others upset.

• immediately inform an adult if I something that worries me, or I know is inappropriate.

• keep my username and password secure; this includes not sharing it with others.

• understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.

• only use my log in and not log in using someone else's name or password

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the school's ICT systems and internet.
I understand that there will be consequences if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):

Date:

Covingham Park Primary School

Parent/Carer agreement

I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

APPENDIX 2 – ACCEPTABLE USE OF PUPIL'S MOBILE PHONE IN SCHOOL HOME-SCHOOL AGREEMENT

Covingham Park Primary School Home-School Agreement
Acceptable use of mobile phones in school agreement for pupils and parents/carers (Years 5 and 6 pupils only)

Dear Parents

Please complete below the reason that your child needs to bring their phone to school.

If the school do not feel that this is a valid reason, then they will contact you to discuss this.

Reason:

Parent/carer agreement:

If the school agree that my child may bring their phone to school for the reason stated above, then I agree to the conditions set out below for pupils bringing mobile phones into school and will make sure my child understands these. I understand that if it is agreed that my child may bring their mobile phone to school, then the school takes no responsibility for any loss or damage to the phone whilst on school property because it is not a piece of required school equipment.

Signed (parent/carer):

Date:

Name of pupil:

If the school agree to allow me to bring my mobile phone to school and I understand that I
- must switch off my mobile phone as I enter school grounds, not in the building.
- must hand my phone to a member of staff when arriving at school, where it will be stored safely.
- must collect my phone at the end of the day.
- must not use my mobile phone in the toilets or changing areas. This is to protect the privacy and welfare of other pupils.
- cannot take photos or recordings (either video or audio) of school staff or other pupils without their consent.

I understand that the school reserves the right revoke permission if I don't abide by the policy.

Signed (pupil):

Date:

I agree/disagree that ..... bring their mobile phone to school for the reason stated above.

Signed (Headteacher):

Date:

APPENDIX 3 - STAFF, GOVERNOR AND VISITOR ACCEPTABLE USE POLICY

IT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT. All staff are expected to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with a member of SLT.

APPENDIX 4 – COMMON TYPES OF CYBER BULLYING

• Text messages — that are threatening or cause discomfort – also included here is "blue jacking" (the sending of anonymous text messages over short distances using "Bluetooth" wireless technology).

• Picture/video-clips via mobile phone cameras – images sent to others to make the victim feel threatened or embarrassed.

• Mobile phone calls — silent calls or abusive messages; or stealing the victims' phone and using it to harass others, to make them believe the victim is responsible.

• Emails — threatening or bullying emails, often sent using a pseudonym or somebody else's name.

• Chatroom bullying — menacing or upsetting responses to children or young people when they are in web-based chatrooms.

• Instant messaging (IM) — unpleasant messages sent while children conduct realtime conversations online using MSM (Microsoft Messenger) or Yahoo Chat.

• Bullying via websites and social networking sites — use of defamatory blogs, personal websites and online personal "own web space" sites.

• The best way to deal with Cyberbullying is to prevent it happening in the first place and to have clear steps to take when responding to it

APPENDIX 5 – FILTERING AND MONITORING

Introduction

Schools in England (and Wales) are required "*to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering*" Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to *"ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT"* however, schools will need to "*be careful that "over*

blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

Ofsted concluded as far back as 2010 that "Pupils in the schools that had 'managed' systems had better knowledge and understanding of how to stay safe than those in schools with 'locked down' systems. Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves."

To further support schools and colleges in England, the Department for Education published Digital and Technology standards.

Roles and Responsibilities

The school and Trust work in partnership with the IT service provider (*Wave9)* to ensure that the school infrastructure/network is as safe and secure as is reasonably possible. DfE Filtering Standards require that schools and colleges identify and assign roles and responsibilities to manage filtering and monitoring systems.

Role	**Responsibility**	**Name / Position**
Responsible Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.	Ray Williams
Senior Leadership	Team Member Responsible for ensuring these standards are met and: • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision • overseeing reports Ensure that all staff: • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns	Joanne Andrews
Designated Safeguarding Lead	Lead responsibility for safeguarding and online safety, which includes overseeing and acting on: • filtering and monitoring reports • safeguarding concerns	Joanne Andrews

	• checks to filtering and monitoring systems	
IT Service Provider	Technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems	Wave 9
All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:	• they witness or suspect unsuitable material has been accessed • they can access unsuitable material • they are teaching topics which could create unusual activity on the filtering logs • there is failure in the software or abuse of the system • there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks • they notice abbreviations or misspellings that allow access to restricted material	

Policy statement

- There is a filtering and monitoring system in place that safeguards staff and learners by blocking harmful, illegal and inappropriate content.
- There is a monitoring system that enables the prompt investigation of a potential safeguarding incident, and outcomes are logged.
- Roles and responsibilities for the management of filtering and monitoring systems have been defined and allocated.
- There is a defined and agreed process for making changes to the filtering or monitoring system that involves a senior leader in the agreement of the change.
- Mobile devices that access the school's internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems.
- The school has provided enhanced/differentiated user-level filtering through the use of the Wave 9 filtering system. (allowing different filtering levels for different ages/stages and different groups of users – staff/learners etc.)

Filtering Procedures

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, as online content changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use.

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and other illegal content lists. There is a clear route for reporting and managing changes to the filtering system. Personal mobile devices are not allowed internet access through the school network.

The filtering system used in our school is up to date and applied to all:

- users, including guest accounts
- school owned devices
- devices using the school broadband connection

This system:-

- filters all internet feeds, including any backup connections
- is age and ability appropriate for the users and is suitable for educational settings
- handles multilingual web content, images, common misspellings and abbreviations
- identifies technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them
- provides alerts when any web content has been blocked
- is regularly updated

Monitoring Procedures

Monitoring user activity on school and college devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software. Monitoring allows review of user activity on school devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing prompt action to be taken.

Our monitoring strategy includes:

- physical monitoring by staff watching screens of users
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon.

Filtering and Monitoring Review and Checks

Strategic review

The filtering and monitoring provision is reviewed at least annually, as part of a wider online safety annual review, using the 360 degree safe tool, or when:

- a safeguarding risk is identified
- there is a change in working practice, e.g. remote access or BYOD
- new technology is introduced

The review is conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the IT service provider.

Operational review

In addition to the annual review of filtering and monitoring, checks to filtering and monitoring systems are completed and recorded as part of the filtering and monitoring review process. How often the checks take place will be based on the context, the risks highlighted in the filtering and monitoring review, and any other risk assessments.

Checks will be undertaken from both a safeguarding and IT perspective.

In our school, we complete the following checks:-

1. a review of the monitoring logs to check for patterns and themes which may arise from user access and cause concern. These are completed termly

2. Checks of the filtering systems are performed on a range of:

- school owned devices and services, including those used off site
- geographical areas across the site
- user groups, for example, teachers, pupils and guests
- Existing pupil log ins are tested for this purpose and after the check browser history is removed so that the pupil is not able to view previous searches.

Logs of checks are kept so they can be reviewed. These record:

- when the checks took place
- who did the check
- what was tested or checked
- resulting actions

A check using the SWGfL Test Filtering website is also completed termly

Changes to Filtering and Monitoring Systems

There should be a clear process for requests to change the filtering and monitoring systems and who makes the decision to alter the filtering system.

In this section the school should provide a detailed explanation of:

- how, and to whom, users may request changes to the filtering and monitoring systems
- the grounds on which changes may be permitted or denied
- how a second responsible person will agrees to the change before it is made

Training/Awareness

It is a statutory requirement in England that staff receive training, at least annually, about safeguarding, child protection, online safety and filtering and monitoring.

Governors, Senior Leaders and staff are made aware of the expectations of them:

- at induction
- at whole-staff/governor training
- through the awareness of policy requirements
- through the acceptable use agreements
- in regular updates throughout the year

Those with specific responsibilities for filtering and monitoring receive enhanced training to help them understand filtering and monitoring systems and their implementation and review.

Learners are made aware of the expectations of them:

- in lessons (the schools should describe how this will take place)
- through the acceptable use agreements

Parents are informed of the school's filtering policy through the acceptable use agreement and through online safety awareness sessions/newsletter etc.

This appendix is informed by the Department for Education (DfE) guidance, Keeping Children Safe in Education, and the Digital and Technology Standards and is based on a template from the South West Grid For Learning (SWGfL).