Roberts Primary School

Online Safety Policy

Revised: Spring Term 2024
Consultation Period: ended March 2024
Approved by Governors: April 2024

Date of Next review: Spring Term 2025

To be read in conjunction with:
Computing Policy
Safeguarding Policy
Behaviour and Safety Policy
Anti-Bullying Policy
Staff Code of Conduct
Teaching Online Safety in Schools (DfE, June 2019)
Whistleblowing Policy
Complaints Policy
Data Protection Policy
Remote Education Code of Conduct
Roberts Primary School Remote Education Policy

Approved by:
Senior Leader - Mrs D Hunt (Headteacher)
Governor - Mrs S Smith (Chair of Governors)

Online safety Advice and Guidance

Rationale

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.

'Safeguarding and promoting the welfare of children is **everyone's** responsibility' (KCSIE).

Scope

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school but are linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action will be taken as specified in our Behaviour Policy.

Schools/Academies who wish to implement Part 2 of the Education Act 2011 (Discipline); the added power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices should ensure that other policies reflect this content. School Electronic Devices - Search and Deletion.

The school will deal with such incidents within this policy and associated Behaviour and Anti-Bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour, that take place out of school.

Development, Monitoring and Review of the Online Safety Policy:

This Online safety policy has been developed by a working group made up of:

- School/Online Safety Coordinator
- Headteacher/Senior Leaders
- Teachers
- Support Staff
- ICT Technical staff
- Governors/Board

Consultation with the whole school community has taken place through the following:

- Staff meetings
- School Council
- INSET Days
- Governors committee meetings
- School website/newsletters

The school will monitor the impact of the policy using**:**

- Logs of reported incidents
- DGfL or internal monitoring logs of internet activity (including sites visited)
- Updates from the LA
- Attendance at DSL briefings
- LA bulletins/managed service bulletins
- Township foci
- Communications from external agencies i.e. the Police, CCG

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Committees, receiving regular information about online safety incidents and monitoring reports - *(It is suggested that Governing Bodies review their online safety policy at the start of each academic year to ensure that all new staff and pupils are aware of its content and have signed appropriate Acceptable Use Agreements-see Appendices 3 and 4).*

The member of the Governing Body responsible for child protection will also take on the role of online safety Governor – Mrs J Morgan

The role of the Online Safety Governor will include:

- Regular meetings with the Online Safety Co-ordinator/Officer (ESO)
- Regular updates on the monitoring of online safety incident logs
- Regular updates on the monitoring of the filtering of web sites
- Reporting to relevant Governor committees/meetings

Headteacher and Senior Leaders:

The Headteacher is responsible for ensuring the safety (including Online Safety) of members of the school community and is likely to be the school's Senior Information Risk Owner (SIRO), Dawn Hunt. The schools SIRO is responsible for reporting security incidents as outlined in the schools Information Security Policy. The day to day responsibility for Online Safety will be delegated to the Senior Leadership Team (SLT) who has this responsibility.

- The Headteacher is responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant. They are also responsible for ensuring that pupils and students are taught how to use ICT tools such as the internet, email and social networking sites, safely and appropriately
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in the school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- The SLT will receive regular monitoring reports from the online safety Co-ordinator.
- The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

  DSPP information: Management of allegations against staff

- The Headteacher is responsible for ensuring that parents and carers, when given access to data and information relating to their child/children via an online communication system, have adequate information and guidance relating to the safe and appropriate use of this online facility https://dudleychildrenservices.sharepoint.com/InformationGovernance/_layouts/15/start.aspx#/
- The Headteacher or a designated member of the SLT is responsible for ensuring that parents/carers understand that the school may investigate any reported misuse of systems, by pupils, out of school hours, as part of 'safeguarding' procedures. This process may be specified in other policies *e.g. Behaviour Policy, Child Protection Policy*

Online Safety Coordinator:

The school has a named person, Ken Hughes, with the day to day responsibilities for Online Safety. Responsibilities include:

- Leading the online safety committee
- Taking day to day responsibility for online safety issues and having a leading role in establishing and reviewing the school online safety policies/online safety documents
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Providing training and advice for staff
- Liaising with the Local Authority, LADO or relevant organisations
- Liaising with the school's SIRO to ensure all school data and information is kept safe and secure
- Liaising with school ICT technical staff and school contact from the managed service provider- RM

- Receiving reports of online safety incidents and creating a log of incidents to inform future online safety developments
- Meeting regularly with the Online Safety Governor to discuss current issues, review incident logs and filtering.
- Attending relevant meetings/Governor committee meetings
- Cascading centrally communicated updates as appropriate
- Reporting regularly to the Senior Leadership Team

Managed service provider (applicable to DGfL3 schools):

The managed service provider is responsible for helping the school to ensure that it meets the online safety technical requirements outlined by DGfL, which is aligned to national guidance. The managed service provides a number of tools to schools including e-Safe, Smoothwall filtering and MDMs (Mobile Device Management systems), which are designed to help schools keep users safe - (see appendix 2).
Schools are able to configure many of these locally or can choose to keep standard settings.
A designated adult can access activity logs for network users and apply 'rules' to specific group of users. Schools should nominate a suitable member of staff to manage this responsibility and keep logs of any changes made to filtering and monitoring rules.
CC4 Anywhere and similar products, are applications that enables a user to remotely access documents and applications stored on the school server/servers. The school has responsibility for ensuring files and applications accessed via this system comply with information and data security practices. Schools may wish to specify the type of information that users can access via CC4 Anywhere or a similar product that allows remote access to the server.

The DGfL Client team work with school representatives to develop and update a range of Acceptable Use Agreements/guidance (see Appendix 3, 4 and 5) and include relevant Local Authority online safety policies and guidance.

http://safeguarding.dudley.gov.uk/child/

http://safeguarding.dudley.gov.uk/child/work-with-children-young-people/education-information/

http://safeguarding.dudley.gov.uk/child/work-with-children-young-people/Online Safety-and-use-of-images/

Members of the DGfL team will support schools to improve their online safety strategy.
The managed service provider maintains backups of email traffic for 90 days. If access to this information is required, the school should contact the DGfL team.

Teaching and Support Staff:

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices
- They have read and understood the most recent guidance specified in KCSIE (Keeping Children Safe in Education-DfE)
- They encourage pupils to develop good habits when using ICT to keep themselves safe
- They have read, understood and signed the school Staff Acceptable Use Agreements (AUA's)
- They report any suspected misuse or problem to the online safety co-ordinator Headteacher
- Digital communications with students pupils (email / Virtual Learning Environment (VLE), applications/O365 Apps/Google Apps / voice) should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum, in line with the statutory 2014 curriculum requirements
- Students / pupils understand and follow the school online safety and acceptable use agreements
- Students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of online safety issues related to the use of mobile phones, cameras and hand held devices, including their personally owned devices and that they monitor their use and implement current school policies with regard to the use of these devices in the school or during extended school activities.
- In lessons, where internet use is pre-planned, students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. They include the teaching of online safety in their lessons
- Pupils understand that there are sanctions for inappropriate use of technologies, including peer on peer abuse, and the school/academy will implement these sanctions in accordance with the AUA or any statements included in other policies e.g. Behaviour Policy, Anti-Bullying Policy
- Pupils understand that the school may investigate any reported misuse of systems, by pupils, out of school hours as part of 'safeguarding' procedures

Designated Person for Child Protection/Child Protection Officer:

The named person, Dawn Hunt, is trained in online safety issues and is aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Publishing of specific information relating to school based activities involving pupils, via official school systems such as the school web site, external school calendar, Twitter, Facebook, You Tube.
- Sharing of school owned devices or personal devices that may be used both within and outside of the school
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming

- Cyber-Bullying, Sexting and Sextortion, Revenge Porn, Radicalisation, CSE (See Child Protection Policy.)

Online Safety Committee:

Members of the online safety committee will assist the online safety coordinator with:

- The production / review / monitoring of the school online safety policy / documents
- The review / monitoring of the managed service filtering policy
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders, including parents, carers and the pupils about the online safety provision
- Identifying current technology trends used out of school

Students/Pupils:

Students/pupils have access to the school network and technologies that enable them to communicate with others beyond the school environment. The network is a secure, monitored and safe system provided through DGfL. Students/pupils:

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Agreement/AUA *(see appendix 3*), which they, will be expected to agree to before being given access to school systems
- Need to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images, use of social networking sites, video streaming facilities, digital image sharing sites and cyber-bullying. This includes the implications of use outside of school
- Are responsible for the safe use of school owned equipment if used at home, in accordance with the school UA, for these devices. The school AUA may be used.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to the use of an externally available web based system, provided by the school
- Should understand that the school has a 'duty of care' to all pupils. The misuse of non-school provided systems, out of school hours, will be investigated by the school in line with our behaviour, anti-bullying and safeguarding policies.

Parents/Carers:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will therefore take every opportunity to

help parents understand these issues through parents' evenings, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature.

Parents and carers will be responsible for:

- Accessing the school website / School Learning Platform/ on-line student / pupil records in accordance with the relevant school Acceptable Use Agreement.
- Promoting good online safety practice by following guidelines on the appropriate use of digital and video images taken at school events and their children's devices in school.

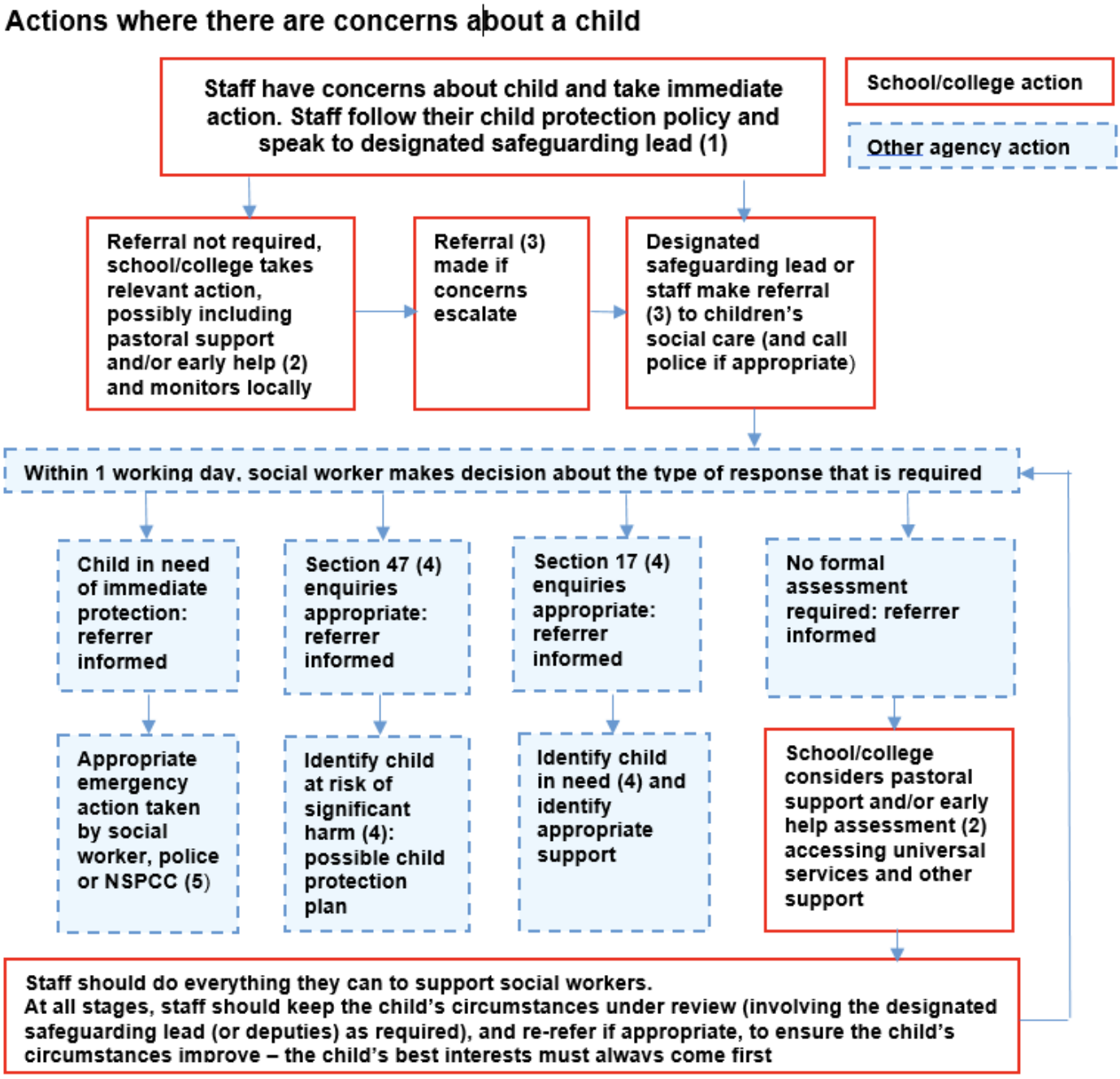
Community Users/'Guest Access':

Community Users who access school ICT systems / website / School Learning Platform/on-line student/pupil records as part of the Extended School provision will be expected to sign a Community User AUA before being provided with access to school systems-see appendix 5.

Reporting Procedures:

Harmful content is anything online which causes a person distress or harm. All staff are aware of sources of support for online safety issues, such as the Professionals Online Safety Helpline, Reporting Harmful Content, CEOP and Internet Watch Foundation.

In all cases if staff have any concerns, they must take immediate action, following the safeguarding policy and talk to one of the school's designated safeguarding leads.



Additional information and guidance	
DGfL Info.Security-Technical Policy	*(available from school computer)*
Dudley - Safe and Sound	https://www.dudleysafeandsound.org/onlinesafety
Online Harms White Paper	https://www.gov.uk/government/consultations/online-harms-white-paper
DfE- Preventing and Tackling Bullying (2017)	https://www.gov.uk/government/publications/preventing-and-tackling-bullying
Keeping Children Safe in Education	https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
Working Together to Safeguard Children	https://www.gov.uk/government/publications/working-together-to-safeguard-children--2
Use of images	http://safeguarding.dudley.gov.uk/child/work-with-children-young-people/online Safety-and-use-of-images/
Safeguarding and Child Protection Policy	http://safeguarding.dudley.gov.uk/child/work-with-children-young-people/education-information/
Searching, Screening and Confiscation at School	https://www.gov.uk/government/publications/searching-screening-and-confiscation
Revised Prevent Duty	https://www.gov.uk/government/publications/prevent-duty-guidance
SWGfL Policy and AUA's	https://swgfl.org.uk/products-services/onlinonline Safety/resources/onlinonline Safety-policy-templates/

Policy Statement

Education – Students/Pupils

There is a planned and progressive online safety/E-literacy curriculum. Learning opportunities are embedded into the curriculum throughout the school and are taught in all year groups. All staff have a responsibility to promote good online/online Safety practices.
online safety education is provided in the following ways:

- A planned online safety/E-literacy programme is provided as part of Computing / PHSE / other lessons (specify) and is regularly revisited – this include the use of ICT and new technologies in and outside the school
- Key online safety messages are reinforced as part of a planned programme of assemblies and pastoral activities
- Students / pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy and plausibility of information
- Students / pupils are aware of the Student / Pupil AUA's and are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside the school
- Students/pupils are aware that their network activity is monitored and where students/pupils are allowed to freely search the internet their internet activity is being scrutinised
- Students/pupils may need to research topics that would normally be blocked and filtered. Any request to unfilter blocked sites for a period of time, must be auditable
- Students / pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet are posted in all rooms and are displayed on log-on screens, specified in separate policies relating to the use of school endorsed systems
- Students and pupils are taught the importance of information security and the need to keep information such as their password safe and secure
- Staff act as good role models in their use of ICT, the internet and mobile devices

Education – Parents/Carers

The school provides information and awareness to parents and carers through:

- Letters, newsletters, school web site, school Learning Platform
- Parents evenings, Nursery/Reception induction meetings
- Online safety sessions for parents/carers
- High profile events or campaigns
- Family learning opportunities

Education - Extended Schools

The school signposts family learning courses in ICT, computing, digital literacy and online safety so that parents/carers and children can together gain a better understanding of these issues. Messages to the public around online safety are targeted towards grandparents and other relatives as well as parents/carers.
Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education & Training – Staff/Volunteers

All staff/volunteers receive regular online safety training and understand their responsibilities, as outlined in this policy. Training is offered as follows:

- A planned programme of formal online safety training is made available to staff. An audit of the online safety training needs of all staff is carried out regularly. It is expected that some staff will identify online safety as a training need within the performance management process
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements
- The online safety Coordinator/DSL (or other nominated person) receives regular updates through attendance at DGfL / LA /LSGB/ other information / training sessions and by reviewing guidance documents released by DfE / DGfL / LA, LSGB and others
- This online safety policy and its updates are presented to and discussed by staff in staff / team meetings / INSET days
- The online safety Coordinator/ DSL provides advice / guidance / training as required to individuals

All staff are familiar with the school policy including:

- Safe use of e-mail
- Safe use of the internet including use of internet-based communication services, such as instant messaging and social network or any other school approved system
- Safe use of the school network, including the wireless network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras
- Publication of pupil information/photographs/videos/posts/blogs/calendars and information available on the school website
- Capturing and storing photographs/videos/audio files on personal and school owned devices
- Cyberbullying procedures
- Their role in providing online safety education for pupils
- The need to keep personal information secure

All staff are reminded / updated about online safety matters at least once a year.

Training – Governors

Governors/Directors take part in online safety training / awareness sessions, particularly those who are members of any sub-committee / group involved in ICT/Computing / online safety / Health and Safety / Child Protection

.

This is offered by:

- Attendance at training provided by the Local Authority / National Governors Association / DGfL/ LSGB or other relevant organisation
- Participation in any school training / information sessions for staff or parents
- Invitation to attend lessons, assemblies and focus days

Technical – infrastructure / equipment, filtering and monitoring

The managed service provider is responsible for ensuring that the school 'managed' infrastructure / network is as safe and secure as is reasonably possible. The school is responsible for ensuring that policies and procedures approved within this document are implemented.

Filtering

DGfL filtering is provided by Smoothwall. The IWF (Internet Watch Foundation) list and the "police assessed list of unlawful terrorist content, produced on behalf of the Home Office", is integrated into the Smoothwall database.

- Web filtering policies are applied based on:
- "who" (user or user group from a directory),
- "what" (type of content),
- "where" (client address – either host, subnet or range),
- "when" (time period) in a filtering policy table that is processed from top-down

Monitoring

DGfL's monitoring solution is provided by e-Safe. e-Safe's detection technology monitors imagery, words and contextual phrases, during online and offline activity, to identify behaviour which may represent a safeguarding risk or breach of acceptable use policies.

School ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the AUA's

- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted to authorised users

All users will have clearly defined access rights to school ICT systems

- All users will be provided with a username and password
- Users will be required to change their password every 90 days using *Password Plus which forces users to change their password and defines the complexity of password required* as being 8 characters, inclusion of a capital letter, lower case letter, number and special character and not having the same password as 3 previous passwords.
- Users will be made responsible for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The school maintains and supports the managed filtering service provided by DGfL.
- The school manages and updates filtering issues through the RM Service desk/SWURL management console
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager/appropriate member of staff (Ken Hughes). If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the online safety Committee
- Remote management tools are used by staff to control workstations and view user's activity
- An appropriate system is in place for users to report any actual / potential online safety incident to the relevant person

- The managed service provider ensures that appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data
- An agreed procedure is in place for the provision of temporary access to "guests" (e.g. trainee teachers, visitors) onto the school system. This is auditable.
- An agreed procedure is in place that explains the equipment is not to be used by anyone who has not been authorised by the school.
- A guardianship document is signed before school owned equipment leaves the premises. This clearly outlines the user's responsibilities.
- An agreed procedure is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off site unless safely encrypted or otherwise secured.
- The school has responsibility for ensuring files and applications accessed via CC4 Anywhere or a similar application, comply with information and data security practices.

Curriculum

Online safety is a focus in all areas of the curriculum. The Computing curriculum specifically identifies 'Digital Literacy' as a focus. Digital Literacy is taught. Staff will re-enforce online safety messages in the use of ICT across the curriculum and during Computing lessons.

- In lessons, where internet use is pre-planned, students / pupils are guided to sites checked as suitable for their use and there are processes in place for dealing with any unsuitable material that is found in internet searches
- Where students / pupils are allowed to freely search the internet, e.g. using search engines, staff should monitor the content of the websites the young people visit
- The school provides opportunities within a range of curriculum areas to teach about online safety
- The school teaches 'Digital Literacy' as part of the new 'Computing' programme of study
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the network manager or managed service provider temporarily remove those sites from the filtered list for the period of study. Any requests to do so are auditable and should be logged
- Students / pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- Students / pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Pupils are aware of the impact of Cyberbullying, Peer on Peer abuse, Sharing of Nude/Semi-nude images (Sexting), Cybercrime, Revenge Porn and Radicalisation and know how to seek help if they are affected by any form of online bullying or exploitation. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button

Use of Digital and Video Images

When using digital images, staff inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital / video images to support educational aims, and follow school policies concerning the storing, sharing, distribution and publication of those images. Those images are only taken on school equipment, the personal equipment of staff are not used for such purposes
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupil's device.
- Care is taken when capturing digital / video images, ensuring students / pupils are appropriately dressed and that they are not participating in activities that might bring the individuals or the school into disrepute
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and comply with good practice guidance on the use of such images
- Students' / pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers is obtained before photographs of students / pupils are published on the school website or on an official school social networking application

  DSCB Guidance/Policies:
  http://safeguarding.dudley.gov.uk/child/work-with-children-young-people/online Safety-and-use-of-images/

- Student's / pupil's work can only be published with the permission of the student / pupil and parents or carers. Parents should have signed the DSCB consent form

- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.

Remote Working: Communicating with Parents, Carers and Pupils

Where education is taking place remotely, it's important for schools, teachers and pupils to maintain professional practice as much as possible.
When communicating online with parents and pupils, staff:

- Communicate within school hours as much as possible (or hours agreed with the school to suit the needs of staff)
- Communicate through the school channels approved by the senior leadership team
- Use school email accounts (not personal ones)
- Use school devices over personal devices wherever possible
- Do not share personal information

Video and Online Conferencing/Lessons:

Recording of video conferences

The ability to record a lesson, tutorial or meeting has many advantages. It can benefit several learning activities, including the delivery of training events, briefings, webinars and the discussions of projects; discussions and content can then be referred to or made available as an ongoing resource.

However, where video conferencing is used (MS Teams), the school considers the following safeguarding points (**NB for the purpose of this, the term participant refers to a child, young person or vulnerable adult):**

- Staff members do not hold one-to-one video conferences with a participant due to safeguarding risk. Where a video conference is required with an individual, two members of staff are present on the video conference
- Staff members work against a neutral background. Staff present themselves as they would if they were giving a face-to-face lesson/ meeting, both in dress and in manner
- The school/academy has an agreed etiquette for video conferencing which is understood by stakeholders (see Remote Education Code of Conduct and Roberts Primary School Remote Education Policy)
- Participants are asked to have a neutral background and present themselves as they would in a face to face lesson/tutorial/meeting and dress appropriately e.g. not in their sleep wear or dressing gowns
- Participants are aware that some video conferencing platforms save a copy of all chat and all conversations (one to one and group), even it is deleted afterwards. Anything written down could be asked for in an information access request
- Where lessons/tutorials are delivered to a class, parents/carers and students are provided with safeguarding and etiquette guidance in advance of the lesson/tutorial e.g. the student should participate in a room with an open door and parents/carers should try and ensure a trusted adult is in the same premises as the student while the lesson takes place
- The school may choose to record the lesson/ meeting if there is a 'lawful basis'. *The legitimate interest needs to take into account the rights and freedoms of the individual and where the participant does not wish to or consent to be recorded, their camera should be switched off. Video conferencing participants should also ensure they have muted their microphone if they do not wish to be recorded*

Where the lessons/meetings are recorded, parents / carers should be informed of:

- The lawful basis for this, which is documented in our Privacy Notice
- The period of time the recording will be kept for
- Where it will be stored
- Who has access to the recording
- Screenshots must not be taken by either staff or participants
- Participants should be reminded that the chat facility on the video conferencing must not be used for personal discussions either during the conference or after
- Where the lesson/tutorial/meeting is recorded with the participants camera on and thus capturing their image, full written parental / carer consent has been sought. Where consent is not given, the lesson/ tutorial/meeting is not recorded if the participant has their camera/microphone switched on

Recording of a video conference is not permitted for some limited matters. If you have any doubts as to whether your video conference will fall under any of the below categories, you should contact your organisations Designated Safeguarding Lead and Data Protection Officer in the first instance for advice.

Call recording is not permitted where the meeting includes discussions about individuals with regards to any of the below. This includes current, former or prospective students, staff or service users:

• Counselling, wellbeing or welfare
• Any disciplinary hearing including those relating to safeguarding

Data Protection

The school has a Data Protection Policy that meets statutory guidance.

Personal data is recorded, processed, transferred and made available according to the current Data Protection Act:

- It has paid the appropriate fee to the Information Commissioner's Office (ICO)
- It has appointed a Data Protection Officer (DPO). The school / academy may also wish to appoint a Data Manager and systems controllers to support the DPO
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified
- Data Protection Impact Assessments (DPIA) are carried out
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers
- Procedures are in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller
- There are clear and understood data retention policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible
- Consideration has been given to the protection of personal data when accessed using any remote access solutions
- The Freedom of Information Policy sets out how FOI requests are actioned

All staff receive data handling awareness / data protection training and are made aware of their responsibilities.
Staff ensure that they:

- Take care at all times, to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Access personal data on secure password protected computers and other devices, at the school/academy and home, or via the school/academy Learning Platform or school/academy systems (delete as appropriate), ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Please refer to guidance available here from Dudley Information Governance:
https://dudleychildrenservices.sharepoint.com/InformationGovernance/_layouts/15/start.aspx#/

Communications

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students / pupils should therefore use only the school email service to communicate with others when in the school, or on school systems e.g. by remote access from home- *(If staff use none standard or personal email accounts these are not secure and cannot always be monitored)*
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and students / pupils or parents / carers (email, chat, school VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. **Personal** email addresses, text messaging or public chat / social networking programmes must not be used for these communications
- Students / pupils are provided with individual school email addresses for educational use
- Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Personal information should not be posted on the school website, on public facing calendars and only official email addresses should be used to identify members of staff
- Mobile phones may be brought into the school by pupils/students but are to be handed into the office daily. A consent form from parents must be signed. At all times the device must be switched off.
- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances should a member of staff contact a pupil or parent/ carer using their personal device unless authorised to do so by the school.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Users bringing personal devices into the school must ensure there is no inappropriate or illegal content on the device
- The school provides a safe and secure way of using chat rooms, blogs and other 'social networking technologies' via a Learning Platform. Other 'social networking' facilities may be 'unfiltered' for curriculum purposes. Staff are aware of the procedure they need to follow when requesting access to externally based social networking sites.

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. The school has a policy that sets out clear guidance for staff to manage risk and behaviour online.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school, through limiting access to personal information:

- Training to include: acceptable use, social media risks, checking of settings, data protection
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and online safety/online safety committee, to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Personal Use:

Personal communications which do not refer to or impact upon the school are outside the scope of this policy. Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken. The school permits reasonable and appropriate access to private social media sites.

Monitoring of Public Social Media:

As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school. The school will effectively respond to social media comments made by others according to a defined policy or process. The school's use of social media for professional purposes will be checked regularly by the senior risk officer and online safety committee, to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable/Inappropriate Activities

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

The school will take all reasonable precautions to ensure online safety is a key focus.
However, owing to the international scale and 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.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview/counselling by online safety/Online Safety Coordinator / Head teacher.
- Informing parents or carers.
- Removal of Internet or computer access for a period, (which could ultimately prevent access to files held on the system)
- Referral to LA SPA
- School policies include infringements relating to online activities (e.g. Behaviour policy, Anti-bullying policy, Child Protection policy)

Our Online Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with school, LSGB child protection procedures.

There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

This Online Safety Guidance and Policy has been written with references to the following sources of information:

Dudley LA
Hertfordshire Online Safety Policy
Kent Online Safety Policies, Information and Guidance
South West Grid for Learning- School Online Safety Policy

DGfL/managed service provider will ask for consent to investigate user account log files (RIPA) and provide information to the designated school contact