QUEEN VICTORIA PRIMARY SCHOOL

E-Safety Policy and Acceptable Use Agreement (AUAs)

Policy Number	39
Policy Date:	June 2021
Review Date:	June 2023
Approved by:	
Date:	14/7/21
Signed by Chair of Governors:	L Ward

QUEEN VICTORIA PRIMARY SCHOOL

Online Safety/E-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).

The E-safety Policy should help to ensure safe and appropriate use. The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks.

The main risks come from

- Addictive use of the internet
- Accessing inappropriate material
- Developing unsafe relationships over the internet
- Bullying and harassment
- Peer on Peer abuse
- Circulation of private information
- Sexting
- Vulnerability to scams

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 school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Head Teachers to such extent as is reasonable, to regulate the behaviour of students 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/e-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.

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 e-safety/online safety behaviour, that take place out of school.

Development, Monitoring and Review of the Online safety/E-Safety Policy:

This E-Safety policy has been developed by the E-Safety Committee

- Schools E-Safety Officer
- Head teacher Senior Leaders
- Teachers
- Support Staff
- ICT Technical staff
- Governors
- Pupils/School Council
- Parents and Carers

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

- Staff meetings
- School/Pupil Council
- INSET Days
- Governors meetings/sub-committee meetings
- Parents evening
- Schools website/newsletters
- The results of surveys/questionnaires with specific reference to e-safety

The schools will monitor the impact of the policy using:

- Logs of reported incidents
- DGfL or internal monitoring logs of internet activity (including sites visited)
- Internal monitoring of data for network activity
- Surveys/questionnaires of stakeholders-including 'pupil voice'
- Updates from the LA
- Attendance at DSL briefings
- LA bulletins/DGfL Gridlines
- Township foci
- Communications from external agencies ie the Police, CCG

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the Online safety/E-Safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors/Full Governing Body Meeting, receiving regular information about online safety/e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online safety/E-Safety Governor

The role of the Online/E-Safety Governor will include:

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

Head teacher and Senior Leaders:

The Head Teacher is responsible for ensuring the safety (including Online safety/E-Safety) of members of the school community and is likely to be the school's Senior Information Risk Owner (SIRO)

The school's SIRO is responsible for reporting security incidents as outlined in the school's Information Security Policy.

- The Head Teacher/SLT have a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Officer. 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 Head Teacher and (at least) another member of the Senior Leadership 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. ***(refer to response and procedures safeguarding incidents see appendix 1)***

http://www.proceduresonline.com/dudley/scb/chapters/p_alleg_against_staff.html#intro

Additional information: http://safeguarding.dudley.gov.uk/report-it/

- The Head Teacher/Senior Leaders are responsible for ensuring that the Online Safety Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

- The Head Teacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles. The Senior Leadership Team will receive regular monitoring reports from the Online Safety Officer.

The SLT will receive regular monitoring reports from the E-Safety Officer. The Head teacher and another member of the SLT should be aware of the procedures to be followed in the event of a serious Online safety /E-Safety allegation being made against a member of staff

http://safeguarding.dudley.gov.uk/child/work-with-children-young-people/management-of-allegations/

- The Head teacher 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 on-line facility- including Queen Victoria Primary School Website and Twitter page. https://dudleychildrenservices.sharepoint.com/InformationGovernance/_layouts/15/start.aspx#/

- The Head teacher or a designated member of the SLT is responsible for ensuring that parents/carers understand that the schools may investigate any reported misuse of systems, by pupils, out of school hours, as part of 'safeguarding' procedures. Refer also to our Positive Behaviour Policy and School Electronic Devices – Search and Deletion Policy.

Online safety/E-Safety Coordinator/Officer:

Mr J Cooke is responsible for the day to day responsibilities of E-Safety.
Mr R Newman is the On-line Safety Governor for the School.

Responsibilities include:

- Leading the Online safety/E-Safety committee
- Taking day to day responsibility for Online safety/E-Safety issues and having a leading role in establishing and reviewing the schools E-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/E-Safety incident taking place
- Providing training and advice for staff
- Liaising with the Local Authority DO (LADO) or relevant organisations
- Liaising with the school's SIRO to ensure all schools data and information is kept safe and secure
- Liaising with school ICT technical staff and/or schools contact from the managed service provider- RM

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

Managed service provider

The managed service provider is responsible for helping the schools to ensure that it meets the Online safety/E-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 Access and similar products, are applications that enable 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 Access or a similar product that allows remote access to the servers.

The DGfL Client team work with school representatives to develop and update a range of Acceptable Use Agreements/guidance *(see Appendix 3)* and include relevant Local Authority Online safety/E-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/e-safety-and-use-of-images/

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

Teaching and Support Staff:

Are responsible for ensuring that:

- They have an up to date awareness of Online safety/E-Safety matters and of the current school Online safety/E-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 schools Staff Acceptable Use Agreements (AUA's)
- They report any suspected misuse or problem to the E-Safety Officer /Head teacher/Senior Leader/DSL for investigation/action/sanction.
- 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/E-Safety issues are embedded in all aspects of the curriculum, in line with the statutory 2014 curriculum requirements
- Pupils understand and follow the school Online safety/E-Safety and acceptable use agreements
- 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/E-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 schools 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/E-Safety in their lessons
- Pupils understand that there are sanctions for inappropriate use of technologies and the schools will implement these sanctions in accordance with the AUA or any statements included in other policies.
- Pupils understand that the schools may investigate any reported misuse of systems, by pupils, out of school hours as part of 'safeguarding' procedures

Designated person for Child Protection/ DSL/ Child Protection Officer:

The named person Mrs C Rindl (Interim) is trained in Online safety/E-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 schools-based activities involving pupils, via official school systems such as the schools web site, external schools calendar, Twitter, Facebook
- Sharing of schools owned devices or personal devices that may be used both within and outside of the schools
- 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

Online safety/E-Safety Committee:

Members of the E-Safety committee will assist the E- Safety Officer with:

- The production/review/monitoring of the school Online safety/E-Safety policy/documents
- The production/review/monitoring of the managed service/schools filtering policy.
- Identifying current technology trends used out of school

Pupils

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.
Pupils:

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Agreement/AUA *(see appendix 3)*, which they, or their parents/carers will be expected to sign 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 schools' policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand schools' 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 schools
- Are responsible for the safe use of schools owned equipment at home, in accordance with the schools AUA, for these devices.

- Should understand the importance of adopting good Online/E-Safety practice when using digital technologies out of school and realise that the school's Online/E-Safety policy covers their actions out of school, if related to the use of an externally available web-based system, provided by the schools
- Should understand that the school has a 'duty of care' to all pupils. The misuse of non-schools provided systems, out of school hours, will be investigated by the schools 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 schools 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/E-Safety campaigns/literature.

Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Agreement
- Accessing the school website/School Learning Platform/on-line Pupil records or other schools provided system (specify here) in accordance with the relevant school Acceptable Use (AUA).
- 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 schools.

Community Users/'Guest Access':

Community Users who access school ICT systems/website/Schools Learning Platform/on-line Pupil records or other schools provided system 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 3.

Additional guidance	
Use of images	http://safeguarding.dudley.gov.uk/child/work-with-children-young-people/e-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 Policies and AUA's	https://swgfl.org.uk/products-services/online-safety/resources/online-safety-policy-templates/

Policy Statement

Education - pupils

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

- A planned Online safety/E-Safety/E-literacy programme is provided as part of Computing/PHSE and is regularly revisited – this include the use of ICT and new technologies in and outside the schools
- Key Online safety/E-Safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- 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
- 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.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Pupils are aware of the Pupil AUA's and are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside the schools
- 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
- Pupils may need to research topics that would normally be blocked and filtered. Any request to un-filter blocked sites, for a period of time, must be auditable
- Rules for use of ICT systems/internet are posted in all rooms and are displayed on log-on screens.
- 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, schools web site, schools Learning Platform, official schools social networking sites
- Parents evenings, Nursery/Reception/induction meetings
- Online/E-Safety sessions for parents/carers
- High profile events or campaigns
- Family learning opportunities
- Curriculum activities

Education - Extended Schools/Wider Community

The school offers family learning courses in ICT, computing, digital literacy and Online safety/E-Safety so that parents/carers and children can together gain a better understanding of these issues. Messages to the public around Online safety/E-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/E-Safety training and understand their responsibilities, as outlined in this policy. Training is offered as follows:

- A planned programme of up to date, formal Online safety/E-Safety training is made available to staff. An audit of the Online safety/ E-Safety training needs of all staff is carried out regularly. Some staff have identified Online safety/E-Safety as a training need within the performance management process
- All new staff receive Online safety/E-Safety training as part of their induction programme, ensuring that they fully understand the school Online safety/E-Safety Policy and Acceptable Use Agreements
- The Online safety/E-Safety Coordinator/DSL (or other nominated person) receives regular updates through attendance at DGfL/LA /LSCB/ other information/training sessions and by reviewing guidance documents released by DfE/DGfL/LA, LSCB and others
- This Online safety/E-Safety policy and its updates are presented to and discussed by staff in staff/team meetings/INSET days
- The Online safety/E-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 schools 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 schools owned devices
- Cyberbullying procedures
- Their role in providing Online safety/E-Safety education for pupils
- The need to keep personal information secure

All staff are reminded/updated about Online/E-Safety matters at least once a year.

Training - Governors

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

.

This is offered by:

- Attendance at training provided by the Local Authority/National Governors Association/DGfL/ LSCB or other relevant organisation
- Participation in schools 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 schools '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.

Schools ICT systems will be managed in ways that ensure that the school meets the Online/E-Safety technical requirements.

- 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 3 months. Passwords to have at least 8 characters containing 1 uppercase, 1 lowercase, 1 number (3 or more consecutive characters from usernames are not allowed)
- FS (Foundation Stage)/SEN pupils/KS1, use a generic password but need to be aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy and the AUAs
- 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
- KS2 users will change their generic passwords to 'strong' passwords.
- Users will lock their computer/laptop if they move away from their working area.
- The school maintains and supports the managed filtering service provided by DGfL. The schools can provide enhanced user-level filtering through the use of Smoothwall filtering.
- The school manages and updates filtering requests through the RM Service desk/Smoothwall management console
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager. If the request is agreed, this action will be recorded, and logs of such actions shall be reviewed regularly by the Online safety/E-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/E-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.

- All executable files are downloaded by the Network Manager or RM Education.
- An agreed procedure is in place regarding the extent of personal use by (staff/students/pupils/community users).
- A guardianship document is signed before schools 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's 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 Access or a similar application, comply with information and data security practices.

Curriculum

Online/E-Safety is a focus in all areas of the curriculum. The new Computing Curriculum specifically identifies 'Digital Literacy' as a focus. Digital Literacy is taught. Staff will re-enforce Online safety/E-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 – The school encourages the use of ICE, a search engine, to ensure pupil's access to the web is safe.
- Where pupils can freely search the internet, e.g. using search engines, staff monitor the content of the websites the young people visit
- The school provides opportunities within a range of curriculum areas to teach about Online/E-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
- 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
- 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, Sexting and Sextortion, 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

Electronic forms of communication have developed rapidly in recent years and the vast majority of children have access to a computer and or mobile phone. Children are frequently exposed to internet abuse including sexual abuse and bullying by phone is on the increase. Any child thought to be the victim of such abuse should therefore be regarded as in need of protection.

Further information can be found in the UKCCIS Guidance: Sexting in schools and colleges, responding to incidents, and safeguarding young people (2016)

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 can 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 is not used for such purposes
- Pupils are not permitted to use personal digital equipment, including mobile phones, smart watches and cameras, to record images of the others, this includes when on field trips. However, with the express permission of the Head teacher, 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 schools 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
- 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's website or on an official schools social networking application (may be covered as part of the AUA and/or Dudley Safeguarding Children's Board-DSCB consent form)
  DSCB Guidance/Policies:
  http://safeguarding.dudley.gov.uk/child/work-with-children-young-people/e-safety-and-use-of-images/

- Pupil's work can only be published with the permission of the Pupil (age appropriate) and parents or carers. Parents/carers 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

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.

Personal data is recorded, processed, transferred and made available according to the Data
Protection Act 2018 includes GDPR which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff are aware of the 'School Information Security Policy'. A breach of the Data Protection
Act may result in the school or an individual fine of up to £500000

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 schools and home, or via the schools Learning Platform or school systems, 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 *(many memory sticks/cards and other mobile devices cannot 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:

Please note the link below is accessible by establishments who have bought into Dudley's Information Governance service.
https://dudleychildrenservices.sharepoint.com/InformationGovernance/_layouts/15/start.aspx#/

Communications

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

- The official schools email service may be regarded as safe and secure and is monitored. Staff and students/pupils should therefore use only the schools email service to communicate with others when in the schools, 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 are 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, schools VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) schools systems. **Personal** email addresses, text messaging or public chat/social networking programmes must not be used for these communications
- Pupils are provided with individual school email addresses for educational use
- 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, smart watches may be brought into the schools by pupils. Parents must complete a consent form which is approved by the Head Teacher.

- Pupils are allowed to bring personal mobile devices/phones/smart watches to school but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent
- 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 schools.
- 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 schools 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 RMUNIFY. 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 schools, 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

Schools staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or schools 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 uses a closed group on Facebook and Twitter page to share information with parents/carers. The rules in the pinned post must be adhered to by all members of the group. The group is monitored by all staff and inappropriate use is reported and dealt with by the administrators of the group. All incidents are recorded in the E-Safety Incident log

- Staff must set up a separate professional account for the group.

- Staff must not add any parents/carers as friends on this account.

All information shared must be through the closed group. The school's use of social media for professional purposes i.e. Facebook and Twitter – will be checked regularly by the senior risk officer & the group administrators 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 authorised staff.
The schools will take all reasonable precautions to ensure Online safety/E-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 tutor/Head of Year/E-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, including examination coursework).
- Referral to LA
- Schools policies include infringements relating to online activities e.g. Behaviour policy, Anti-bullying policy, Child Protection policy.

Our Online safety/E-Safety Coordinator/DSL acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head Teacher.

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

Microsoft Teams

Digital technologies have become integral to the lives of children and young people. These technologies are powerful tools which open up new opportunities including the offer of pastoral and academic support for students. Technologies and digital platforms such as Microsoft Teams can provide opportunities for discussion, promote creativity and stimulate awareness of contextualised subjects to provide effective support for pupils based on their individual pastoral and academic needs.

Young people should have an entitlement to safe internet access at all times.

This Section in relation to Student Acceptable Use is intended to ensure:

• that young people will be responsible users and stay safe while using the internet and other digital technologies to interact with Queen Victoria Primary School.

• that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Queen Victoria Primary School staff will primarily use Microsoft Teams as a communication tool to support students for academic purposes if school closure continues for a prolonged period of time.

Gaining access to Microsoft Teams
To gain access to Microsoft Teams every student will be provided with an email address and a password. The email address will act as the student's Office 365 log-on name. Once logged on students can access the Teams icon within this software.

The email address will also allow students to access and use the school email system which can also be found on the Office 365 homepage. Both platforms are monitored and neither should be considered 'private' by students.

Students are responsible for their own accounts and are expected to follow the Online Safety rules taught in lessons when interacting on Microsoft Teams including (but not exclusive to):

• Never revealing private information including date of birth, home addresses or contact details.

• Never distribute images of themselves of others via Microsoft Teams.

• Using appropriate words and actions when participating in calls and chats.
Students are strongly advised never to share their log-on name or password with anybody other than their trusted adults within their home environment.

Microsoft Teams in a 'Live' format
'Live' interactions to support students will always be initiated by a staff member who will make contact with students prior to the interaction starting to advise a start date

and time. Students are expected to log onto Microsoft Teams around five minutes prior to this time to be ready to accept the call request.

Staff will inform all students when the interaction has finished and all students will log off Microsoft Teams immediately to allow the staff member to close the call.
Student behaviour when participating within a 'Live' interaction will mirror normal classroom behaviour.

Students will be expected to:

• Respect all participants by allowing others to share their view point in a safe environment.

• Respond to questions or tasks from staff members in an appropriate way.

• Attempt all tasks in a positive manner.

• Engage with enthusiasm when collaborating virtually with class members.

Remote Interactions using Microsoft Teams
For Microsoft Teams to be used effectively and safely, students must agree to the following points:

• Students must not use Microsoft Teams to call, chat or set up groups between each other or with any staff and parents.

• Students must not attempt to start or record a meeting.

• Students must not share any resources, recorded videos, PowerPoints, assemblies or other materials uploaded by staff or other students within or outside of Queen Victoria Teams accounts.

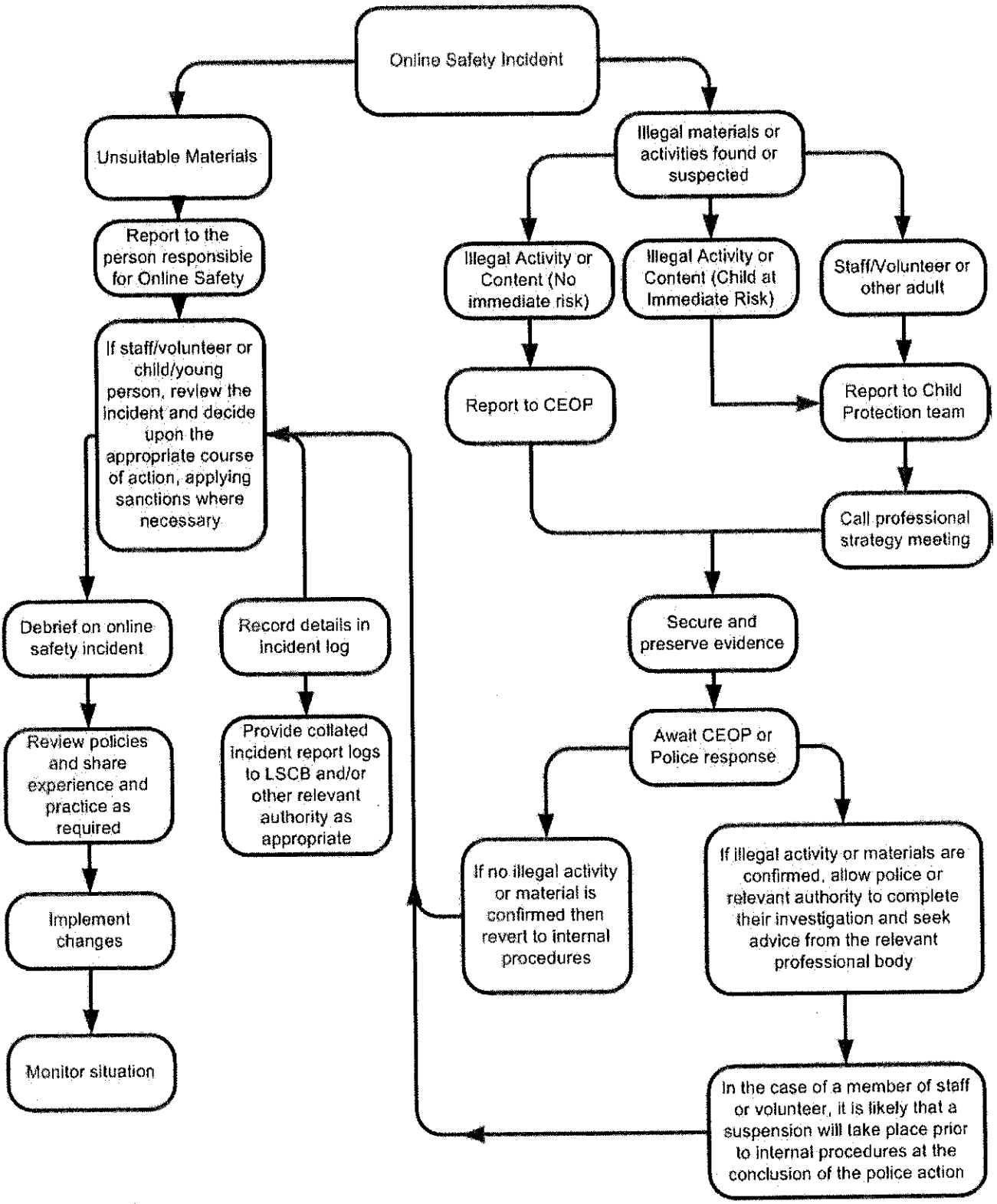
• Students must think carefully about what is acceptable language with regards to what they say, type or post when using Microsoft Teams. This includes the use of emoji's and images.

• Students must hang up at the end of the interaction or when instructed to do so.

School to family interactions have had to be made at a distance since the Covid-19 outbreak and require teachers and students to adapt normal classroom routines to the online world. It is an expectation the normal high levels of behaviour expected when in school will remain in place at all times when interacting with the school from home.

Policy Review Date June 2023
Contact: Mr James Cooke

Appendix 1- E-Safety/Online



Appendix 2-E-Safety/Online safety tools available on the DGfL network

E-Safety tool	Type	Availability	Where	Details
Smoothwall filtering	Web filtering	Provided as part of DGfL	All network connected devices within DGfL	Gives schools the ability to audit, filter and un-filter websites
RM Tutor	Teacher support	Provided as part of DGfL	Managed school desktops	Allows teachers to view and demonstrate screens, control hardware and distribute work
CC4 AUA	Awareness raising	Part of CC4- needs to be enabled	All CC4 stations at log in	When enabled through the management console, users are given an acceptable use policy at log in
eSafe	Monitoring software- *licenses available on Windows, Apple Mac*	Available to all schools	All school desktops and networked laptops, Chrome books and Apple Mac networks	Takes a snapshot of a screen when an event is triggered. A range of events can be monitored. Reports are sent to designated staff in school
Email	Filtering and list control	Provided as part of DGfL	Office 365	Allows schools to restrict where email is sent from/to
DGfL 'Security Enhancements'	Safe practice	Provided as part of DGfL3	All CC4 stations	A password management policy that enforces password rules of complexity and length for different users

Staff/Volunteer Acceptable Use Agreements are intended to ensure that:

- staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- staff are protected from potential risk in their use of technology in their everyday work

Pupil Acceptable Use Agreements are intended to ensure that:

- young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use
- school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *students/pupils* to agree to be responsible users

When forming a pupil AUA, you may want to consider statements that focus on:

- For my own personal safety
- Understanding that everyone has equal rights to use technology as a resource
- Acting as I expect others to act toward me
- Understanding that I am responsible for my actions both inside and outside of the educational establishment

Best practice indicates that pupils involved in formulating AUA's have a greater awareness of the importance of adhering to the agreed principles.

Community Users Acceptable Use Agreements are intended to ensure that:

- community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- users are protected from potential risk in their use of these systems and devices

Appendix 3 - Primary pupil AUA for KS1 and electronically

Queen Victoria Primary School

Acceptable Use Agreement (AUA) for children

When I log on I agree that:

I will only use my own username and password to log on. I will keep my password secret.

I will only use websites that have been suggested by the teacher or a grown up.

I will not give out personal information; tell people where I live, my phone number or where I go to school without permission from the teacher/parent.

I will always ask an adult before sharing photos. I will only share photos that I don't mind everyone seeing.

I will tell a grown up if I feel scared or unhappy about anything I find when using the school computers/laptops.

I will respect school property; I will use the internet, computers and laptops and all other equipment properly.

Appendix 3 - Primary pupil AUA

Queen Victoria Primary School

Rules for Responsible Internet Use

For Primary Pupils

The school has installed computers and provided Internet access to help our learning. I understand that the school may check my computer files and may monitor any Internet sites I visit.

These rules will keep everyone safe and help us to be fair to others. It is important that you read this policy carefully. If there is anything that you do not understand, please ask.

I agree that:

I will not share any of my passwords with anyone, or use another person's password. If I find out someone else's password, I will tell that person and a member of the school staff, so they can change it.

I will use a password which contains some small and some big (capital) letters plus a number or a symbol *e.g. Skool5 or com**2er* and change it on a regular basis.

I will use the technology at school for learning. I will use the equipment properly and not interfere, change or delete someone else's work.

If I use a flash drive or other storage device, I will follow school guidelines on their use.

I will only e-mail people I know, or my teacher has approved.

If I attach a file to an email, it will not include any inappropriate materials (something I would not want my teacher to see or read) or anything that threatens the integrity of the school ICT system.

I will be respectful in how I talk to and work with others online and never write or participate in online bullying. If anyone sends me a message, I do not like or feel uncomfortable about I will show it to my teacher or parent.

I will report any unpleasant material or messages sent to me. I understand my report would be confidential and would help protect other pupils and myself.

I will not download any programmes or games on to the school computers, netbooks or laptops unless I have permission to do so.

I will always check with a responsible adult before I share or publish images of myself, my friends or other people onto the internet.

I will not make audio or video recordings of another pupil or teacher without their permission.

When using sites on the internet, I will not give my name, home address, telephone/mobile number, pretend to be someone else or arrange to meet someone I do not know, unless my parent, carer or teacher has given permission.

I will always follow the 'terms and conditions' when using a site. The content on the web is someone's property and I will ask my teacher to help me get permission if I want to use information, pictures, video, music or sound files.

I will think carefully about what I read on the Internet, question if it is from a reliable source and use the information to help me answer any questions (I should not copy and paste the information and say it's my own work).

If I want to connect my own device to the school network, I will check with my teacher to see if it is possible.

I am aware of the CEOP report button and know when to use it.

I know anything I do on the computer may be seen by someone else.

Signed: .....

PRINT NAME: .....

Dated: .....

Appendix 3 - Staff AUA

QUEEN VICTORIA PRIMARY SCHOOL

Staff Acceptable Use Agreement

Rules for Responsible Internet use

This policy applies to all adult users of the school's systems. We trust you to use the ICT facilities sensibly, professionally, lawfully, consistent with your duties, with respect for your colleagues and in accordance with this Policy.

It is important that you read this policy carefully. If there is anything that you do not understand, please discuss it with the Head Teacher or your line manager. Once you have read and understood this policy thoroughly, you should sign this document, retain a copy for your own records and return the original to the Head Teacher

Any inappropriate use of the School's internet & e-mail systems whether under this policy or otherwise may lead to disciplinary action being taken against you under the appropriate disciplinary procedures which may include summary dismissal. Electronic information can be produced in court in the same way as oral or written statements.

Research Machines (RM) has a contractual obligation to monitor the use of the internet and e-mail services provided as part of DGfL, in line with The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Traffic data and usage information may be recorded and may be used in disciplinary procedures if necessary. RM, Dudley MBC and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request. If there is any evidence that this particular policy is being abused by individuals, we reserve the right to withdraw from employees the facility to view, send and receive electronic communications or to access the internet.

All information relating to our pupils, parents and staff is personal. You must treat all school information with the utmost care whether held on paper or electronically.

Official school systems must be used at all times.

Use of the Internet and Intranet

When entering an internet site, always read and comply with the terms and conditions governing its use. Be aware at all times that when visiting an internet site, the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying your school. For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

- unauthorised access to computer material i.e. hacking;
- unauthorised modification of computer material; and
- unauthorised access with intent to commit/facilitate the commission of further offences.

In line with this policy, the following statements apply: -

- If you download any image, text or material check if it is copyright protected. If it is then follow the school procedure for using copyright material.
- Do not download any image, text or material which is inappropriate or likely to cause offence. If this happens accidentally report it to a senior member of staff.
- If you want to download any software, first seek permission from the Head Teacher and/or member of staff responsible /RM. They should check that the source is safe and appropriately licensed.
- If you are involved in creating, amending or deleting web pages or content on the web site, such actions should be consistent with your responsibilities and be in the best interests of the School.
- You should not:
    - introduce packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;
    - seek to gain access to restricted areas of the network;
    - knowingly seek to access data which you are not authorised to view;
    - introduce any form of computer viruses;
    - carry out other hacking activities.

Electronic Mail

Care must be taken when using e-mail as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school. Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your head teacher. Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the School's business purposes which include the following:

1. providing evidence of business transactions;
2. making sure the School's business procedures are adhered to;
3. training and monitoring standards of service;
4. preventing or detecting unauthorised use of the communications systems or criminal activities;
5. maintaining the effective operation of communication systems.

In line with this policy the following statements apply: -

- You should agree with recipients that the use of e-mail is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted e-mail is not secure.
- Do not send sensitive personal data via email unless you are using a secure site or portal. It is good practice to indicate that the email is 'Confidential' in the subject line.
- Copies of emails with any attachments sent to or received from parents should be saved in a suitable secure directory.
- Do not impersonate any other person when using e-mail or amend any messages received.

- Sending defamatory, sexist or racist jokes or other unsuitable material via the internet or email system is grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making such comments verbally or in writing.
- It is good practice to re-read e-mail before sending them as external e-mail cannot be retrieved once they have been sent.
- If the email is personal, it is good practice to use the word 'personal' in the subject header and the footer text should indicate if it is a personal email the school does not accept responsibility for any agreement the user may be entering into.
- Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your Head Teacher.
- All aspects of communication are protected by intellectual property rights which might be infringed by copying. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights.

Social networking

The use of social networking sites for business and personal use is increasing. Access to social networking sites is blocked on the school systems, however a school can manage access by un-filtering specific sites, internet usage is still monitored.

School staff may need to request access to social networking sites for a number of reasons including:

- Advertising the school or managing an 'official' school presence,
- For monitoring and viewing activities on other sites
- For communication with specific groups of adult users e.g. a parent group.

Social networking applications include but are not limited to:

- Blogs
- Any online discussion forums, including professional forums
- Collaborative spaces such as Wikipedia
- Media sharing services e.g. YouTube, Flickr
- 'Microblogging' applications e.g. Twitter

When using school approved social networking sites, the following statements apply:
-

- School equipment should not be used for any personal social networking use
- Staff must not accept friendships from underage pupils. The legal age for students to register with a social networking site is usually 13 years; be aware that some users may be 13 or younger but have indicated they are older
- It is important to ensure that members of the public and other users know when a social networking application is being used for official school business. Staff must use only their @<schoolname>. dudley.sch.uk email address or other school approved email mechanism and ensure all contributions are professional and uphold the reputation of the school

- Social networking applications should not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- Postings should not be critical or abusive towards the school, staff, pupils or parents or used to place a pupil, student or vulnerable adult at risk of harm
- The social networking site should not be used for the promotion of personal financial interests, commercial ventures or personal campaigns, or in an abusive or hateful way
- Ensure that the appropriate privacy levels are set. Consider the privacy and safety settings available across all aspects of the service – including photos, blog entries and image galleries. Failing to set appropriate privacy levels could result in messages which are defamatory, libellous or obscene appearing on your profile before you have chance to remove them
- It should not breach the schools Information Security policy

Data protection

The processing of personal data is governed by the Data Protection Act 1998. Schools are defined in law as separate legal entities for the purposes of complying with the Data Protection Act. Therefore, it is the responsibility of the School, and not the Local Authority, to ensure that compliance is achieved.
As an employee, you should exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of the School. The main advantage of the internet and e-mail is that they provide routes to access and disseminate information.

Through your work personal data will come into your knowledge, possession or control. In relation to such personal data whether you are working at the School's premises or working remotely you must: -

- keep the data private and confidential and you must not disclose information to any other person unless authorised to do so. If in doubt, ask your Head Teacher or line manager;
- familiarise yourself with the provisions of the Data Protection Act 1998 and comply with its provisions;
- familiarise yourself with all appropriate school policies and procedures;
- not make personal or other inappropriate remarks about staff, pupils, parents or colleagues on manual files or computer records. The individuals have the right to see all information the School holds on them subject to any exemptions that may apply.

If you make or encourage another person to make an unauthorised disclosure knowingly or recklessly you may be held criminally liable.

I have read through and fully understand the terms of the policy. I also understand that the school may amend this policy from time to time and that I will be issued with an amended copy.

Signed: .....

PRINT NAME .....

Dated: ..... .

QUEEN VICTORIA PRIMARY SCHOOL

Community User- Acceptable Use policy

Rules for Responsible Internet use

This policy applies to all community users of the school's systems, who have guest access to the internet. We trust you to use the ICT facilities sensibly, professionally, lawfully, and in accordance with this Policy.

It is important that you read this policy carefully. If there is anything that you do not understand, please ask. Once you have read and understood this policy thoroughly, you should sign this document, retain a copy for your own records and return the original to the school office.

Research Machines (RM) has a contractual obligation to monitor the use of the internet and e-mail services provided as part of DGfL, in line with The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Traffic data and usage information may be recorded and RM, Dudley MBC and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request.

When entering an internet site, always read and comply with the terms and conditions governing its use. Be aware at all times that when visiting an internet site, the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying our school. For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

- unauthorised access to computer material i.e. hacking;
- unauthorised modification of computer material; and
- unauthorised access with intent to commit/facilitate the commission of further offences.

In line with this policy, the following statements apply: -

- Do not download any image, text or material which is copyright protected without the appropriate authorisation.
- Do not download any image, text or material which is inappropriate or likely to cause offence. If this happens accidentally report it to a member of staff
- If you want to download any software, first seek permission from the member of staff responsible. They should check that the source is safe and appropriately licensed.
- You should not:
    - introduce packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;
    - seek to gain access to restricted areas of the network;
    - knowingly seek to access data which you are not authorised to view;
    - introduce any form of computer viruses;

I have read through and fully understand the terms of the policy. I also understand that the school may amend this policy from time to time and that I will be issued with an amended copy.

Signed: .....

PRINT NAME .....

Dated: .....

Appendix 4: Staff guardianship loan form

QUEEN VICTORIA PRIMARY SCHOOL

Portable ICT Equipment – Staff Guardianship Loan Form

Name ..... has permission to loan and is guardian of the following item(s) of ICT equipment: -

Item	Serial No	Start date	Return date

Whilst the above items are in your care, the school will expect you to take full personal responsibility for the safe custody of all of the items listed and to follow the guidelines below: -

- I will ensure the mobile device is secured or locked away when not in use;
- I will ensure that unauthorised software is not loaded or run on this mobile device;
- I will not download, store or collect any inappropriate material on the device
- I will ensure that all external media sources (discs, USB flash drives/memory sticks) are checked for viruses before data transfer to the mobile device where appropriate;
- I will ensure the device is regularly virus-checked where appropriate;
- I will ensure the Anti-virus- software, where appropriate, is kept up to date;
- I will ensure that data remains confidential and secure;
- Where personal data about staff or pupils, or school confidential data, is stored on the device, the device will be encrypted and password protected (as appropriate to the device), and the data will be removed as soon as reasonably possible
- I will ensure that the equipment is not used by anyone who has not been authorised by the school
- I will return the device upon request and when I am on leave or other absence, unless otherwise authorised.
- I will ensure the equipment is not left unattended in any vehicle (as this is not covered by the school's insurance policy), and accept that any loss arising from a loss from a vehicle will be my own responsibility.
- If the equipment is lost or stolen, I will inform the police as soon as possible to get a crime number and also contact the appropriate member of staff

Signed ..... Date .../.../...

Name person authorising the loan .....

Signed ..... Date .../.../...

Appendix 4: Pupil guardianship loan form (adapt/amend as appropriate)

QUEEN VICTORIA PRIMARY SCHOOL

Portable ICT Equipment – Pupil Guardianship Loan Form

Name ..... has permission to loan and is guardian of the following item(s) of ICT equipment: -

Item	Serial No	Start date	Return date

Whilst the above item is in your care, the school will expect you to take full personal responsibility for the safe custody of this item and to follow the guidelines below: -

- I will look after the device. I will ensure it is secured or locked away when not in use;
- I agree to use it sensibly. I will ensure that unauthorised software is not loaded or run on this mobile device;
- I will not download, store or collect any inappropriate material on the device
- I will ensure that all external media sources (discs, USB flash drives/memory sticks) are checked for viruses before data transfer to the mobile device where appropriate;
- I will ensure the device is regularly virus-checked where appropriate;
- I will ensure that data remains confidential and secure;
- Any personal data stored on the device will be encrypted if appropriate and removed as soon as reasonably possible
- I will ensure that the equipment is not used by anyone who has not been authorised by the school
- I will return the device upon request and when I am on leave or other absence, unless otherwise authorised.
- I will ensure the equipment is not left unattended in any vehicle (as this is not covered by the school's insurance policy), and accept that any loss arising from a loss from a vehicle will be my own responsibility.
- If the equipment is lost or stolen, I will inform the police as soon as possible to get a crime number and also contact the appropriate member of staff

Parents' Consent Form

I give permission for my son/daughter _____ to receive a ..... for the duration of the project.

Signed ..... (Parent/Carer)

Name person authorising the loan .....

Signed ..... Date .../.../...