Dawley Brook Primary School

Dubarry Avenue, Kingswinford

DY6 9BP, 01384 818770

Updated: August 2023

ONLINE SAFETY POLICY

2023 - 2024

Ofsted Good Provider

Historic England Champion Heritage School

School Games Gold 2018/19

School Member of Music Mark – Committed to high quality music education

Management and Update of the Policy

Last Reviewed/Revised	Date	Next Review Date	Designated Safeguarding Lead	Deputy Designated Safeguarding Leads	Safeguarding Governor
September 2022 (Revision)	August 2023	August 2024	Mr M. Walters	Ms. L. Maskell	Mrs Angela McHenry

MANAGEMENT AND UPDATE OF THE POLICY

Responsibility for the monitoring of this policy: Dawley Brook Primary School Governing Board

This policy is linked directly to National Legislation and DSPPB thresholds and operating procedures. In addition, it has been written with references to the following sources of information: Hertfordshire E-Safety Policy, Kent e-Safety Policies, Information and Guidance, South West Grid for Learning- Online Safety School template Policies.

Our Online Safety Policy is a living document and will be updated in response to changes in legislation or DSPPB operating procedures (This will occur at least once on an annual basis)

All staff and stakeholders may contribute to the development of our policies and procedures.

Our policy will be published on our website and paper copies are available upon request.

Contents

Safeguarding Definition

Safeguarding and promoting the welfare of children is defined for the purposes of this guidance as:

- protecting children from maltreatment;
- preventing impairment of children's mental and physical health or development;
- ensuring that children grow up in circumstances consistent with the provision of safe and effective care; and
- taking action to enable all children to have the best outcomes.

(The term children, includes everyone under the age of 18.)

Safeguarding is what we do for all children and young people to keep them safe whilst in our care. Child protection describes the policy and procedures specifically for those young people who are at risk of serious harm or have been seriously harmed.

At Dawley Brook Primary School we are committed to safeguarding children and young people and we expect everyone who works in our school to share this commitment.

Adults in our school take all welfare concerns seriously and encourage children and young people to talk to us about anything that may worry them. We will always act in the best interest of the child.

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/academies are bound.

Scope

This policy applies to all members of the school community (including staff, 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 Headteachers ,to such extent as is reasonable, to regulate the behaviour of 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 community.

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 Online Safety behaviour, that take place out of school.

Development, Monitoring and Review of the Online Safety Policy:

Dawley Brook Primary School's Online Safety Policy has been developed by a committee made up of:

- Designated Safeguarding Lead
- Head teacher/Senior Leaders
- Teachers
- Pupils
- Support Staff
- ICT Technical staff
- Governors
- Parents and Carers
- Community users

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

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

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)
- Internal monitoring of data for network activity
- Surveys / questionnaires of stakeholders including 'pupil voice'
- Updates from the LA and DSPP (Dudley Safeguarding People Partnership)
- Attendance at DSL briefings
- LA bulletins/managed service bulletins
- Township foci
- Communications from external agencies i.e. the Police, CCG

Roles and Responsibilities: Governing Board:

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 Health and Safety Working Party before being approved at Standards Committee. This committee will also receive regular information about online safety incidents and monitoring and filtering reports.

A member of the Governing Board has taken on the role of Online safety Governor.

The Online Governor is **Angela McHenry** (Link Governor responsible for Child Protection and Safeguarding)

The role of the Online Safety Governor will include:

- Regular meetings with the Designated Safeguarding Lead;
- Regular updates on the monitoring of Online safety incident logs;
- Regular updates on the monitoring of the filtering of web sites/change control logs;
- Reporting to the Full Governing Body on a termly basis;
- Strategic responsibility for reviewing the effectiveness of filtering and monitoring systems, at least annually;
- Attendance at Online safety meetings, conference, training.

Dawley Brook Primary School's Governing Board ensures that all governors receive appropriate safeguarding and child protection (including online) training at induction. This includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

Roles and Responsibilities: Headteacher and Senior Leaders:

- The Headteacher has 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/Designated Safeguarding Lead.
- 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).
- The school's SIRO is responsible for reporting security incidents as outlined in the school's Information Security Policy.
- The Headteacher and Deputy Headteacher are 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/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. This includes ensuring enhanced online safety training can be provided for the Designated Safeguarding Lead and others who support them in their role; this includes filtering and monitoring systems.
- The Headteacher/Senior Leaders are responsible for ensuring safeguarding training for staff, including online safety and cyber security training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning.
- The Headteacher/Senior Leaders are responsible for ensuring roles and responsibilities for the management of filtering and monitoring systems are assigned to staff and all staff understand their role and responsibilities.
- The Headteacher/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 and filtering reports from the Online Safety Officer.
- 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 on-line facility. The school will have a record of their chosen online systems and associated privacy notices.
- The Headteacher or a designated member of the Senior Leadership Team 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.

Roles and Responsibilities: Designated Safeguarding Lead

At Dawley Brook Primary School, the role of Designated Safeguarding Lead is included within the wider responsibilities of The Designated Safeguarding Lead.

The Designated Safeguarding Lead is **Mr M. Walters** (Deputy Headteacher)

Specific responsibilities related to the day to day management of Online Safety at the school include:

- Taking day to day responsibility for Online Safety issues and having a leading role in establishing and reviewing the school Online Safety policies/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;
- 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/or school contact from the managed service provider (DGfL and 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;

The Designated Safeguarding Lead is trained in identifying 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 Dawley Brook Primary School's web site, external school outlook calendar, Twitter (X) etc;
- 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 including potential or actual incidents of grooming;
- Cyber-bullying, Peer on peer abuse, Sharing of Nude/Semi-nude images (Sexting) and Sextortion, Revenge porn, Up skirting, Radicalisation, CSE, CCE, Cybercrime.

The designated safeguarding lead takes lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).

Roles and Responsibilities: Managed service provider:

- The managed service provider is responsible for helping Dawley Brook Primary School to ensure that it meets the Online Safety technical requirements outlined by DGfL, which is aligned to national guidance, including the filtering and monitoring standards.

- The managed service provides a number of tools to schools/academies including Smoothwall Monitor, RM SafetyNet filtering and MDMs (Mobile Device Management systems), which are designed to help Dawley Brook Primary School keep users safe *(see appendix 2)*. The school can configure many of these locally or can choose to keep standard settings.

- The Senior Leadership Team 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.

- The nominated members of staff for Dawley Brook Primary School are Ms. L. Maskell (Headteacher) and Mr M.Walters (Deputy Headteacher).

- Any changes to filtering and monitoring databases are considered, to ensure there is no unreasonable impact on teaching and learning.

- CC 4Access and similar products, are applications that enable a user to remotely access documents and applications stored on the school servers. Dawley Brook Primary School has responsibility for ensuring files and applications accessed via this system comply with information and data security practices.

- 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 policies and guidance.

- Members of the DGfL team will support Dawley Brook Primary School 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 nominated member of staff for Dawley Brook Primary School should contact the DGfL team.

Roles and Responsibilities: Teaching and Support Staff:

Are responsible for ensuring that:

- They have an up to date awareness of Online Safety matters and of Dawley Brook Primary School's Online Safety policy and practices, including responsibilities in relation to filtering and monitoring and how to escalate concerns when identified.
- They have read and understood the most recent guidance specified in Keeping Children Safe in Education 2023;
- They have read, understood and signed the school Staff Acceptable Use Agreements (AUA's);
- They encourage pupils to develop good habits when using ICT to keep themselves safe;
- They report any suspected misuse or problem to the Online Safety Officer or Headteacher for investigation as appropriate;
- Digital communications with pupils (email, video conferencing, applications etc.) 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 and RSE statutory guidance;
- Pupils understand and follow the school Online Safety Policy and Acceptable Use Agreements (AUAs);
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- They monitor computing 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 or wearable devices that have the capability of connecting via 4G/5G, 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, 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;
- Pupils understand that there are sanctions for inappropriate use of technologies, including peer on peer abuse, and the school will implement these sanctions in accordance with the AUA or any statements included in other policies;
- Pupils understand that the school may investigate any reported misuse of systems, by pupils, out of school hours as part of 'safeguarding' procedures.

Roles and Responsibilities: Community Users or 'Guest Access':

Community Users who access Dawley Brook Primary School's ICT systems e.g. network, internet, website, School PING or other school provided system as part of the Extended School provision, will be expected to sign a Community User Acceptable Use Agreement before being provided with access to the systems.

Guest access to the internet in Dawley Brook Primary school will be subject to the same filtering rules as other school users.

Roles and Responsibilities: Pupils

Pupils have access to Dawley Brook Primary School's network and technologies that enables them to communicate with others beyond the school environment. The network is a secure, monitored and safe system. As such pupils:

- Are responsible for using the school computing systems in accordance with the Pupil Acceptable Use Agreement *(see appendix 3*), which they, or their parents/carers will be expected to sign before being given access to school systems;
- Should know that school owned devices have monitoring and filtering systems installed, that captures information and blocks access to specific websites. Reports from both systems will be scrutinised;
- 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, hand-held and wearable 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 Dawley Brook Primary School;
- As appropriate, are responsible for the safe use of school owned equipment at home, in accordance with the school Acceptable Use Agreement, for these devices and upon completion of a guardianship/loan form.
- Should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that this 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 the behaviour, anti-bullying, child protection and other safeguarding policies.

Roles and Responsibilities: 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. Dawley Brook Primary School will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the school website and through the provision of information about national/local Online Safety campaigns or literature.

Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Agreement;
- Accessing the Dawley Brook Primary School website or other school provided system e.g. School PING;
- 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;
- Should know that school owned devices have monitoring and filtering systems, that captures information and blocks access to specific websites. Reports from both systems will be scrutinised by designated staff, as part of safeguarding procedures

Additional information and guidance	
DGfL Info.Security *(available from school computer)*	http://www.dudley.rmplc.co.uk/proposed/CMS/index.php/category/information-security/
Dudley- Safe and Sound	https://www.dudleysafeandsound.org/onlinesafety
DfE- Meeting Digital and Technology Standards in Schools and Colleges	https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges
Teaching Online Safety in Schools	https://www.gov.uk/government/publications/teaching-online-safety-in-schools
DfE- Preventing and Tackling Bullying	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	https://dudleysafeguarding.org.uk/children/parents-and-carers/online-safety-and-use-of-images/
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/online-safety/
DfE Guidance	https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes
Cyber Security Training	https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools

Education: Pupils

Learning opportunities about Online Safety are embedded into the curriculum throughout the school and are taught in all year groups.

All staff have a responsibility to promote good Online Safety practices.

At Dawley Brook Primary School, education about Online Safety is provided in the following ways:

- A planned Online Safety programme is provided as part of, but not limited to, the wider Computing and PHSE curriculum and is regularly revisited. This includes the use of ICT and new technologies in and outside of Dawley Brook Primary School;
- Key Online Safety messages are reinforced as part of a planned programme of assemblies and 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 to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Pupils are supported in building resilience, including 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 Acceptable Use Agreement's and are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside of Dawley Brook Primary School;
- Pupils are aware that their network activity is monitored and where pupils are allowed to freely search the internet, their internet activity is being captured and available for scrutiny;
- 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;
- Pupils are taught the importance of information security, cyber 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

Dawley Brook Primary School provides information and awareness to parents and carers through:

- Letters, newsletters, school web site, official school social networking sites;
- Parents evenings, Nursery/Reception induction meetings;
- Online Safety sessions for parents/carers;

We may share information with parents and carers relating to online challenges and hoaxes and where to get help and support, without exposing children and young people to scary or distressing content.

Education & Training: Staff/Volunteers

All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues.

All staff/volunteers receive regular Online safety training and understand their responsibilities in relation to filtering and monitoring, as outlined in this policy.

Training is offered as follows:

- A planned programme of up to date, formal Online Safety training is made available to staff.
- 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 including an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring;
- The Designated Safeguarding Lead receives regular updates through attendance at Designated Safeguarding Lead Forums and by reviewing guidance documents released by DfE, DGfL, LA, DSPP and others;
- This Online Safety policy and its updates are presented to and discussed by staff in staff meetings and INSET days;
- The Designated Safeguarding Lead provides advice, guidance and training as required to individuals.

All staff are familiar with the school policy including:

- Filtering and Monitoring systems and associated escalation procedures;
- That they should make a report when:
    - they witness or suspect unsuitable material has been accessed;
    - they can access unsuitable material;
    - teaching topics that could create unusual activity on the filtering logs;
    - there is failure in the software or abuse of the system;
    - there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks;
    - they notice abbreviations or misspellings that allow access to restricted material.
- 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;

Education & Training: Staff/Volunteers cont.

- 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/academy owned devices
- Cyberbullying procedures;
- Their role in providing Online Safety education for pupils;
- The need to keep personal information secure.

All staff are formally updated about Online Safety matters and Cyber Security at least once a year.

Training: Governors

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

This is offered by:

- Attendance at training provided by the Local Authority / National Governors Association / DGfL/ DSPP or other relevant organisation;
- Participation in school training/information sessions for staff or parents/carers;
- 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 RM SafetyNet. 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 this 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 Smoothwall. Smoothwall'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.

- 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/academy ICT systems

All users will be provided with a username and password (Year 1– Year 6). Users will be required to change their password at least annually or as is deemed appropriate by the Designated Safeguarding Lead e.g. following a suspected cyber attack or personal security breach. Dawley Brook Primary School have implemented the 'DGfL Security Enhancements' which includes a policy to force users to change their password regularly and can define the level/complexity of password required.

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.

Dawley Brook Primary School maintains and supports the managed filtering service provided by DGfL. The school can provide enhanced user level filtering through the use of RM SafetyNet filtering or MDMs (Managed Mobile Device systems). Changes to filtering and monitoring databases are ratified by The Senior Leadership Team, and are auditable and the reason for these changes is recorded. The audit trail is reported to governors via The Health and Safety Working Party/Standards Committee.

The school manages and updates filtering requests through the RM Service desk/ RM SafetyNet management console.

Requests from staff for sites to be removed from the filtered list will be considered by the Headteacher. 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 procedure is in place for users to report any actual/potential Online safety concerns to the relevant person. This is understood by all stakeholders.

The managed service provider ensures that appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, 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.

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 / hard drive / 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 Access 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.

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 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 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 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, 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

https://dudleysafeguarding.org.uk/children/parents-and-carers/online-safety-and-use-of-images/

When using digital images, staff inform and educate 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;
- Care is taken when capturing digital/video images, ensuring pupils are appropriately dressed and that they are not participating in activities that might bring the individuals or the school into disrepute;
- Pupils must not take, use, share, publish or distribute images of others without their permission;
- Photographs published on the website, or elsewhere that include 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 pupils are published on the school website or on an official school social networking application;
- Pupil's work can only be published with the permission of the pupil and parents or carers. Parents/carers should have signed the DSPP consent forms;
- 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 is 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 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.

Dawley Brook Primary School has its own Remote Learning Policy which outlines whole school procedures in light of a period of school closure.

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, Dawley Brook Primary School considers the following safeguarding points:

- 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;
- The school has an agreed etiquette for video conferencing which is understood by stakeholders;
- 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 e.g. not in their sleep wear or dressing gowns and in manner;
- 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/tutorial/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/tutorials/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

Dawley Brook Primary 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.
- The school has paid the appropriate fee to the Information Commissioner's Office (ICO);
- The school has appointed a Data Protection Officer (DPO). The school may also wish to appoint a Data Manager and systems controllers to support the DPO;
- The 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;
- The school 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 and home, or via 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*;*
- 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.

Communications

When using communication technologies, Dawley Brook Primary School considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and 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. 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 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;

- Pupils are provided with individual school email addresses for educational use. Dawley Brook Primary School may choose to use group or class email addresses for younger age groups e.g. for members of the Early Years Foundation Stage;

- 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;

- Pupils are allowed to bring personal mobile devices/phones/smart watches into the 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 school;

- The school is not responsible for the loss, damage or theft of any personal mobile device;

- The sending of inappropriate text messages, images and videos 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 or similar system.

Social Media: Protecting Professional Identity

All schools/academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Dawley Brook Primary School has an additional Social Media policy that sets out clear guidance for staff to manage risk and behaviour online.

Dawley Brook Primary 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

Dawley Brook Primary School staff should ensure that:

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

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.

Dawley Brook Primary 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.

Dawley Brook Primary 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 authorised staff.

Dawley Brook Primary 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 unacceptable use and possible sanctions.

Sanctions available include:

- Interview/counselling by Designated Safeguarding Lead or 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 or external support agencies.

Dawley Brook Primary School policies include infringements relating to online activities e.g. Behaviour policy, Anti-bullying policy, Child Protection policy.

Our Designated Safeguarding Lead acts as first point of contact for any safeguarding concern. These are dealt with in accordance with Dawley Brook Primary School and Dudley Safeguarding People Partnership Board (DSPPB) procedures.

Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

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.

Acceptable Use Agreements (AUAs)

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;
- Dawley Brook Primary 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.

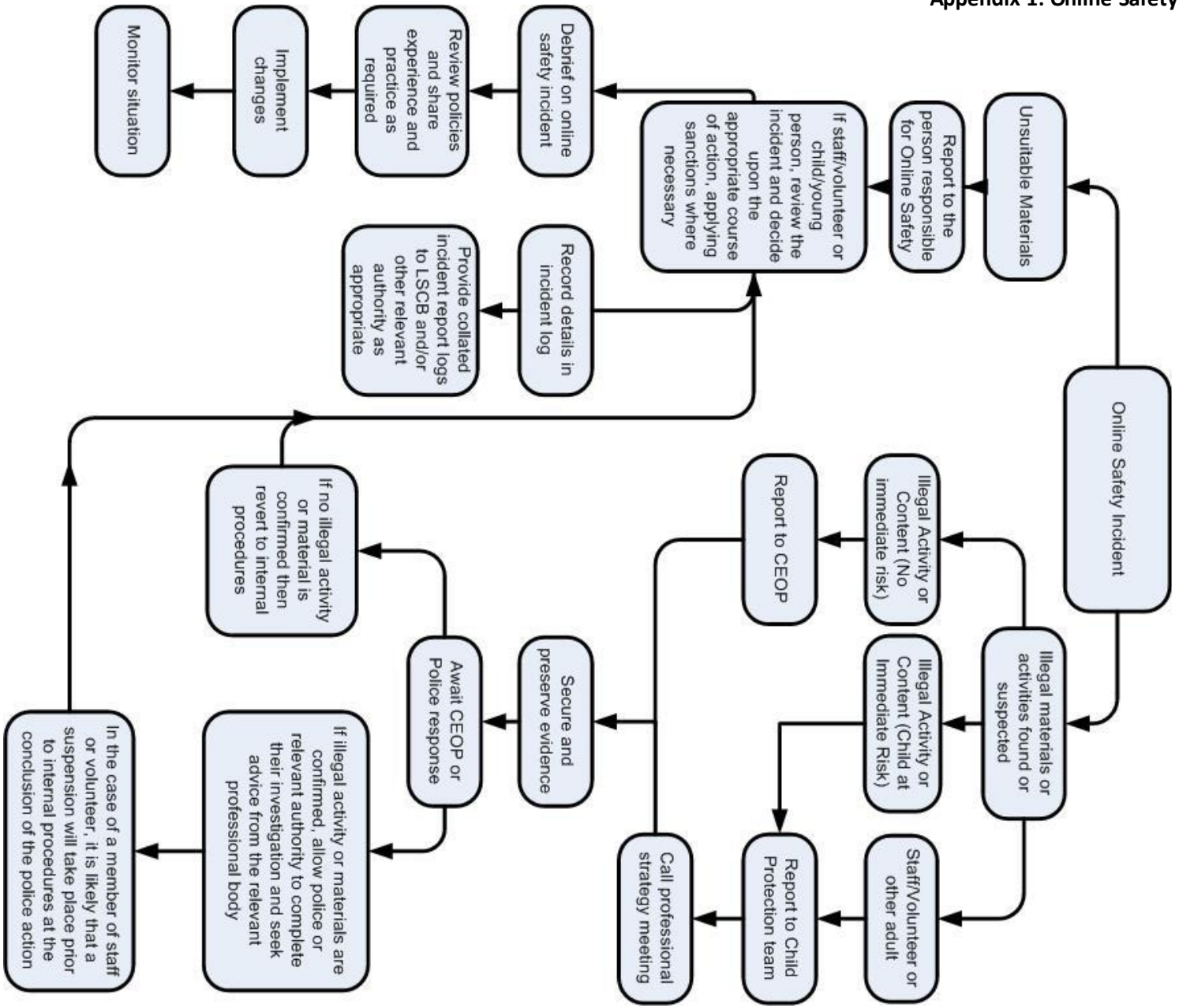
Pupil Acceptable Use Agreements are intended to ensure that:

- 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 pupils to agree to be responsible users;
- Pupils understand that everyone has equal rights to use technology as a resource;
- Pupils understand that I am responsible for my actions both inside and outside of the educational establishment.

Community Users Acceptable Use Agreements are intended to ensure that:

- Community users of Dawley Brook Primary School digital technologies will be responsible users and stay safe while using these systems and devices;
- Dawley Brook Primary 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 1: Online Safety Response Flowchart



Online Safety tool	Type	Availability	Where	Details
RM SafetyNet	Web filtering	Provided as part of DGfL	All network connected devices within DGfL	Gives schools the ability to audit, filter and un-filter websites
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
Smoothwall Monitor	Monitoring software-licenses available on Windows, Chrome books Apple	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 accessed via a secure portal
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