Maidensbridge Primary School

E-Safety Policy

As a Rights Respecting School, we recognise that this policy complies with articles 5, 6, 12, 13, 14, 15, 16 17, 19, 28, 29, 30, 31, 32, 34, 35, 36 & 39 of the United Nations Convention on the Rights of the Child.

May 2021
Review May 2022
Version 2
Reviewed May 2022
Version 3 approved by Governors on 3.5.2022
To be reviewed May 2023
Reviewed September 2023
Version 4 approved by Governors on 6.10.23

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/academies are bound.

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

Scope

This policy applies to all members of the school community (including staff, 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 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 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 Cyber-bullying Policy and Relationships Policy.

The policy is underpinned by the provisions of the General Data Protection Regulations and Data Protection Act 2018

The instigation of this policy follows the guidance set out in the General Data Protection Regulations.

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

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

This E-Safety policy has been developed by a working group made up of:

- School E-Safety Coordinator
- Head Teacher / Senior Leaders
- Teachers
- Support Staff
- ICT Technical staff
- Governors

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
- Attendance at DSL briefings
- LA bulletins/DGfL Gridlines
- Communications from external agencies ie the Police, CCG

Roles and Responsibilities

Governors/Board of Directors:

Governors are responsible for the approval of the E-Safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Core Group, receiving regular information about e-safety incidents and monitoring reports.

The governing board should make sure the designated safeguarding lead (DSL) takes responsibility for understanding the filtering and monitoring systems and processes in place as part of their role (paragraph 103)

The board should also make sure all staff understand their expectations, roles and responsibilities around filtering and monitoring as part of their safeguarding training (paragraph 124)

Governing boards should review the DfE's filtering and monitoring standards. Your board should discuss with your IT staff and service provider what needs to be done to support your school in meeting the standards (KCSIE 23 paragraph 142)

A member of the Governing Board has taken on the role of E-Safety Governor. (Deb Green)

The role of the E-Safety Governor will include:

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

Head Teacher/Principal and Senior Leaders:

The Head Teacher is responsible for ensuring the safety (including 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 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 Lead.

- 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.

  Online Safety and use of images (dudley.gov.uk)

- The Head Teacher / Senior Leaders are responsible for ensuring that the Online Safety Lead 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 filtering and monitoring roles. The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead. The Headteacher receives reports via Smoothwall of any inappropriate activity on all devices in school.

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

  Management of Allegations- Allegations Against Staff (dudley.gov.uk)

- 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.
- 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 school may investigate any reported misuse of systems, by pupils, out of school hours, as part of 'safeguarding' procedures.

E-Safety Coordinator:

The school has a named person with the day-to-day responsibilities for E-Safety which is Mrs R Nicholls (K Thomas while on maternity leave)
Responsibilities include:

- Taking day to day responsibility for E-Safety issues and having a leading role in establishing and reviewing the school E-Safety policies documents
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an E-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- RM

- Receiving reports of E-Safety incidents and creating a log of incidents to inform future E-Safety developments
- Meeting regularly with the 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 (applicable to DGfL3 school):

The managed service provider is responsible for helping the school to ensure that it meets the E-Safety technical requirements outlined by DGfL, which is aligned to national guidance. The managed service provides a number of tools to schools/academies including e-Safe, Smoothwall filtering and MDMs (Mobile Device Management systems), which are designed to help schools/academies keep users safe -*(see appendix* 2).
Schools/Academies can 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/Academies 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/Academies 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 server.

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 E-Safety policies and guidance.

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

Online Safety and use of images (dudley.gov.uk)

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

Teaching and Support Staff:

Are responsible for ensuring that:

- They have an up to date awareness of E-Safety matters and of the current school 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 school Staff Acceptable Use Agreements (AUA's)
- They report any suspected misuse or problem to the Online safety Co-ordinator / Head Teacher / DSL for investigation / action / sanction
- Digital communications with 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
- 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 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 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 school or during extended school activities.
- A guardianship/loan form is available for schools to adapt for school owned equipment used by staff (see appendix).
- 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. They include the teaching of E-Safety in their lessons
- Pupils understand that there are sanctions for inappropriate use of technologies and the school will implement these sanctions in accordance with the AUA or any statements included in other policies- e.g. Behaviour Policy, Anti bullying Policy
- Pupils understand that the school may investigate any reported misuse of systems, by pupils, out of school hours as part of 'safeguarding' procedures

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

Mrs R Nicholls and Mrs K Thomas are trained in E-Safety issues and are aware of the potential for serious child protection issues to arise from:

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

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. 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 school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking / use of images, use of social networking sites, video streaming facilities, digital image sharing sites and cyber-bullying. This includes the implications of use outside of school
- Are responsible for the safe use of school owned equipment at home, in accordance with the school 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 E-Safety policy covers their actions out of school, if related to the use of an externally available web-based system, provided by the school
- Should understand that the school has a 'duty of care' to all pupils. The misuse of non-school provided systems, out of school hours, will be investigated by the school in line with our behaviour, anti-bullying and safeguarding policies.

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national and local Online/E-Safety campaigns and literature.

Parents and carers will be responsible for:

- Endorsing (by signature) the Student / Pupil Acceptable Use Agreement – see appendix 3
- Accessing the school website or other school provided system in accordance with the relevant school 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 school.

Community Users / 'Guest Access':

Community Users who access school ICT systems, website or other school 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	
DGfL Info.Security-Technical Policy *(available from school computer)*	http://www.dudley.rmplc.co.uk/proposed/CMS/index.php/gdpr/ Digital safeguarding software | eSafe Global
Use of images	Online Safety and use of images (dudley.gov.uk)
Safeguarding and Child Protection Policy	Safeguarding children procedures (dudley.gov.uk)
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
Cyberbullying Advice	Bullying and Online Safety (dudley.gov.uk)
Safeguarding in Education	Safeguarding children procedures (dudley.gov.uk)
Remote Learning Policy	DfE external document template (primarysite-prod-sorted.s3.amazonaws.com)

Policy Statement

Education –Pupils

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

- A planned E-Safety 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 school
- Key E-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. **This is taught with reference to the 4Cs (Content, Contact, Conduct and Commerce)**
- 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 (extreme views), 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 Student / Pupil AUA's and are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside the school
- Pupils are aware that their network activity is monitored and where 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 unfilter blocked sites, for a period of time, must be auditable and will have to be done by RM
- Rules for use of ICT systems / internet are posted in all rooms
- 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
- Due to the pandemic, we now have a successful Remote Learning policy in place, where children work on Microsoft Teams.
- Working safely online is reinforced each day and children are aware of how to keep themselves and others safe on the internet.

Education – parents / carers

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

- Letters, newsletters, web site and school social networking sites
- Parents evenings, Reception induction meetings
- Online/E-Safety sessions for parents/carers through the National Online Safety programme
- High profile events or campaigns
- Family learning opportunities
- Curriculum activities

- How to guides to keep children safe when using Teams.

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 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.

Maidensbridge has been awarded the National Online Safety Award.

Education & Training – Staff/Volunteers

All staff/volunteers receive regular 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 E-Safety training is made available to staff. An audit of the E-Safety training needs of all staff is carried out regularly. Some staff have identified E-Safety as a training need within the performance management process
- All new staff receive /Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Acceptable Use Agreements
- The E-Safety Coordinator/DSL (or other nominated person) receives regular updates through attendance at DGfL / LA /LSCB training sessions and by reviewing guidance documents released by DfE / DGfL / LA, LSCB and others
- E-Safety policy and its updates are presented to and discussed by staff in staff / team meetings / INSET days
- /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 school approved system
- Safe use of the school network, including the wireless network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras
- Publication of pupil information/photographs/videos/posts/blogs/calendars and information available on the school website
- Capturing and storing photographs/videos/audio files on personal and school owned devices
- Cyberbullying procedures
- Their role related to filtering and monitoring systems in school and who to talk to if there is an issue
- Their role in providing E-Safety education for pupils
- The need to keep personal information secure

- Remote learning policy and the staff guide on how to keep safe when working from home when using Teams inline with the safeguarding policy.
- Staff are advised, during Remote learning, 1:1 calls are not recommended and only small groups of about 5 children or more are to be conducted.
- Staff are asked to consider location and dress code when carrying out their live lessons.

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

Training – Governors

Governors take part in E-Safety training / awareness sessions, particularly those who are members of any sub-committee involved in ICT/Computing /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 and through The National Online Safety Programme
- Participation in school training / information sessions for staff or parents
- Invitation to attend lessons, assemblies and focus days

Technical – infrastructure / equipment, filtering and monitoring

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

Filtering
DGfL filtering is provided by Smoothwall. The IWF (Internet Watch Foundation) list and the "police assessed list of unlawful terrorist content, produced on behalf of the Home Office", is integrated into the Smoothwall database.
Web filtering policies are applied based on:
"who" (user or user group from a directory),
"what" (type of content),
"where" (client address – either host, subnet or range),
"when" (time period) in a filtering policy table that is processed from top-down

Monitoring
DGfL's monitoring solution is provided by 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.
The Headteacher and E-Safety lead receives regular emails to update on the protection of the devices.

School 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 term.
- Users will be made responsible for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The school maintains and supports the managed filtering service provided by DGfL. The school can provide enhanced user-level filtering through the use of Smoothwall filtering or a MDMs (Managed Mobile Device system)
- 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.
- 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 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. This is auditable
- An agreed procedure is in place regarding the downloading of executable files by users
- An agreed procedure is in place regarding the extent of personal use that users (staff) and their family members are allowed on school owned laptops and other portable devices that may be used out of the school.
- A guardianship document is signed before school owned equipment leaves the premises. This clearly outlines the user's responsibilities
- An agreed procedure is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices
- The school infrastructure and individual workstations are protected by up to date virus software
- Personal data cannot be sent over the internet or taken off site unless safely encrypted or otherwise secured
- The school has responsibility for ensuring files and applications accessed via CC4 Access or a similar application, comply with information and data security practices.

Curriculum

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

- In lessons, where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and there are processes in place for dealing with any unsuitable material that is found in internet searches
- Where 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, pupils 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 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
- Pupils are taught how to use Microsoft Teams correctly and sensibly. They are aware of the use of emojis during chats can offend others and should only use them when instructed to do so by their teachers.
- Pupils are aware of what to do or who to speak to if something does not seem right on their remote learning platform.
- Pupils are taught with knowledge of the 4Cs (Content, Contact, Conduct and Commerce) these are the vulnerabilities and risks of online safety.

Use of digital and video 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

  DSPP Guidance/Policies:
  Online Safety and use of images (dudley.gov.uk)

- 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 DSPP 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 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 2018 and personal data is not retained any longer than is necessary.

The school must ensure that:

It has a Data Protection Policy

- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO). The school may also wish to appoint a Data Manager and systems controllers to support the DPO.
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be 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.
- All schools / academies must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- 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 the school 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:

https://dudleychildrenservices.sharepoint.com/InformationGovernance/_layouts/15/start.aspx#/

Communications

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in the school, or on school systems e.g. by remote access from home- *(If staff use none standard or personal email accounts these are not secure and cannot always be monitored)*
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and pupils or parents / carers (email, School life 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

- 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 and Internet connected smart watches may not be brought into the school by pupils
- Pupils in Year 6 are allowed to bring smart phones to school as long as they are handed-in into the Class teacher at the beginning of the school day. (see Mobile Device Policy).
- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances should a member of staff contact a pupil or parent/ carer using their personal device unless authorised to do so by the school.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Users bringing personal devices into the school must ensure there is no inappropriate or illegal content on the device
- The school provides a safe and secure way of using chat rooms, blogs and other 'social networking technologies' via the school's Office 365 facilities.
  Other 'social networking' facilities may be 'unfiltered' for curriculum purposes. Staff are aware of the procedure they need to follow when requesting access to externally based social networking sites

Social Media - Protecting Professional Identity

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

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

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

School staff should ensure that:

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

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

Unsuitable / inappropriate activities

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000. The school will take all reasonable precautions to ensure 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 E-Safety Coordinator 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 MASH team
- School policies include infringements relating to online activities e.g. Behaviour policy, Anti-bullying policy, Child Protection policy

Our E-Safety Coordinator 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 school, LSCB child protection procedures.

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

Date the Policy was approved by Governors: 6.10.23

Date for review: 1.9.2024

Contact: K Thomas/R Nicholls

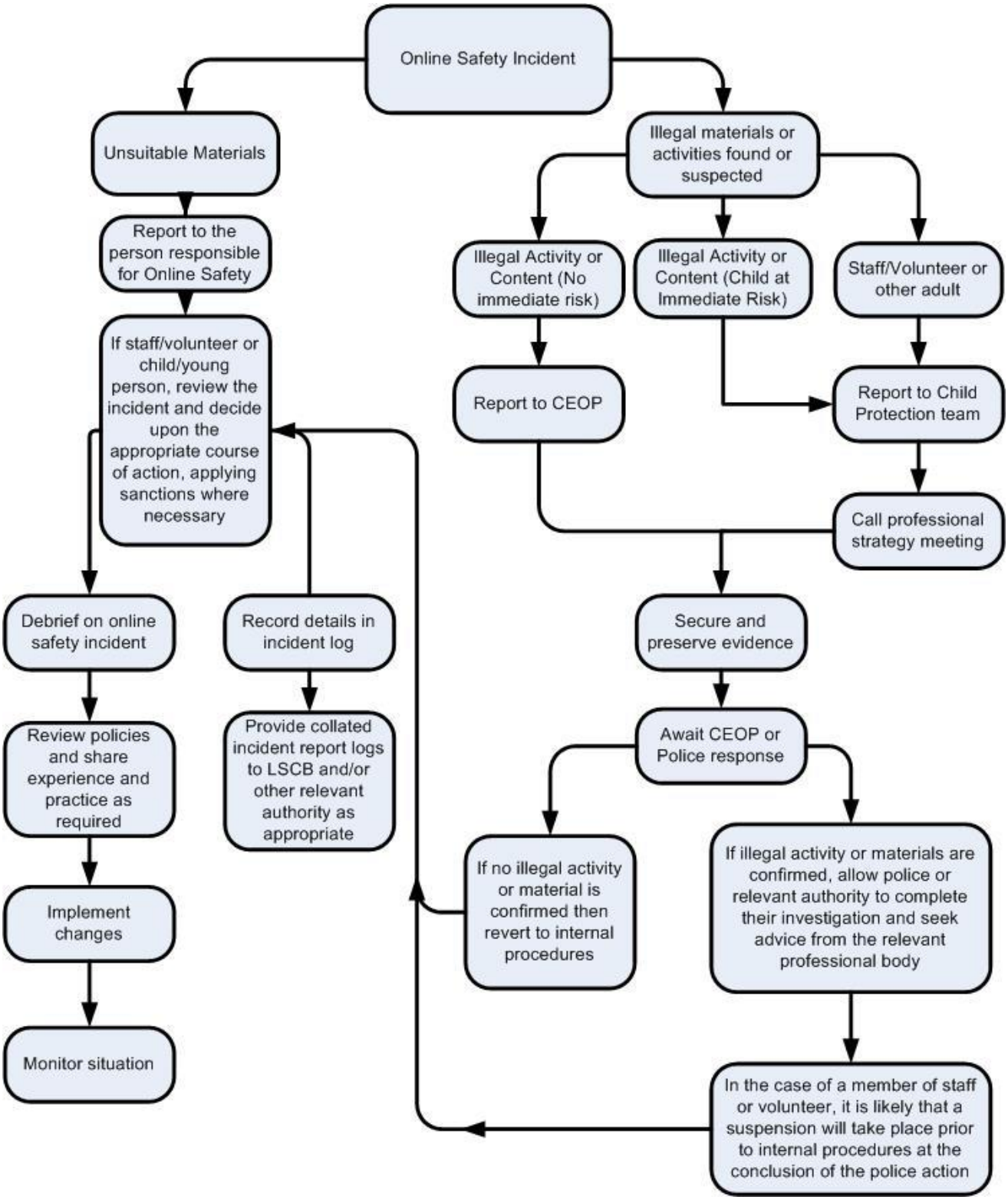
This E-Safety Guidance and Policy has been written with references to the following sources of information:

Dudley LA
Hertfordshire E-Safety Policy
Kent e-Safety Policies, Information and Guidance
South West Grid For Learning- Online Safety School template Policies

Appendix 1- E-Safety sample response

N.B This needs to reflect the educational establishments response and procedures to 'safeguarding' incidents

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



Appendix 2-E-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
Smoothwall	Monitoring software-*licenses available on Windows, Apple Mac*	Available to all schools	All school Windows 7 or 8.1 desktops and networked laptops 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

Appendix 3- Acceptable use of the internet: agreement for pupils and parents/carers (The Key)

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson)
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Share my password with others or log in using someone else's name or password
- Bully other people

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

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

I will always be responsible when I use the school's ICT systems and internet.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):	**Date:**

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

Signed (parent/carer):	**Date:**

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: Sample Staff guardianship loan form

Maidensbridge 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: Sample Pupil guardianship loan form (adapt/amend as appropriate)

Maidensbridge 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/Guardian)

Name person authorising the loan ……..

Signed ……. Date …/…/…