LIVING LIFE IN ALL ITS FULLNESS

St. Margaret's at Hasbury C of E Primary School

(SMAHPS)

Online safety/E safety Policy

Online safety/E safety Policy		
Responsibility for monitoring this Procedure:		
Sara Shepherd and the Governors *(Reviewed annually or in response to changes in legislation or operating procedures)*		
Approved by	Governors	October 2023
Last review on:	October 2023	
Next review due by:	September 2024	

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).

This policy applies to all members of the school (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school's 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/e-safety incidents covered by this policy, which may take place outside of the school but are linked to membership of the school.

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

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

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

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

This Online safety/E-Safety policy has been developed with support from the local authority safeguarding advisor, local authority online safety advisor and developed by the headteacher. This policy will be monitored by headteacher and governors and reviewed in line with statutory changes.

The policy has been shared with all staff during the annual safeguarding training or during induction. A copy is on the school website for parents/carers to read and a link is added to the October school newsletter and on the behaviour policy.

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

- Filtering and monitoring logs
- DGfL or internal monitoring logs of internet activity (including sites visited)
- 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

Governors/Board of Directors:

Governing bodies and proprietors should ensure that all governors and trustees receive appropriate safeguarding and child protection (including online) training at induction.
This should include an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

Governors are responsible for the approval of the Online safety/ E-Safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors, receiving regular information about online safety/e-safety incidents *including, monitoring and filtering reports-*

A member of the Governing Body has taken on the role of Online safety Governor
The role of the Online/E-Safety Governor will include:

- Regular meetings with the Online safety/E-Safety Co-ordinator / Officer (ESO)/ *DSL*
- Regular updates on the monitoring of Online safety/E-Safety incident logs
- Regular updates on the monitoring of the filtering of web sites/change control logs
- Reporting to relevant Governor/ Boards/ committees / meetings
- *Strategic responsibility for reviewing the effectiveness of filtering and monitoring systems, at least annually*
- Attendance at Online safety meetings, conference, training

Head teacher and Senior Leaders:

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

The school's SIRO is responsible for reporting security incidents.

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, and the day-to-day responsibility for online safety.

- The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

  DSPP information: Management of allegations against staff

- The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Officer / Lead/ *DSL* 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 Headteacher / Senior Leaders are responsible for 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. Headteacher will receive support from Jane Dickens and Heather Jeavons.
- The SLT will receive regular monitoring reports, *including filtering reports,* from the Headteacher.
- The SLT/SMT will ensure *all* staff have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively and know *how/who to escalate concerns when identified, in accordance with policy and procedures.*

- 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-
(The Information Security Policy/Data Protection Policy contains detailed guidance). The school will have a record of their chosen online systems and associated privacy notices.

- The Head teacher 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. (see Behaviour policy

Online safety/E-Safety Coordinator / Officer:

The school/academy has a named person with the day-to-day responsibilities for Online safety/E-Safety. Responsibilities include:

- Leading the Online safety/E-Safety committee
- Taking day to day responsibility for Online safety/E-Safety issues and having a leading role in establishing and reviewing the school/academy E-Safety policies / Online safety documents
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an Online safety/E-Safety incident taking place
- Providing training and advice for staff
- *Liaising with the DSL to review filtering and monitoring reports, safeguarding concerns, checks to filtering and monitoring systems* (assuming the Online Safety lead isn't the lead DSL)
- Liaising with the Local Authority/ relevant body
- Liaising with the school's SIRO to ensure all school data and information is kept safe and secure
- Liaising with school's ICT technical staff and school's contact from the managed service provider- RM
- Receiving reports of Online safety/E-Safety incidents and creating a log of incidents to inform future E-Safety/Online safety developments.
- Meeting regularly with the Online safety/E-Safety Governor to discuss current issues, review incident logs and filtering
- Attending relevant meetings / Governor committee meetings
- Cascading centrally communicated updates as appropriate
- Reporting regularly to the Senior Leadership Team

Managed service provider (applicable to DGfL schools):
The managed service provider is responsible for helping the school to ensure that it meets the Online safety/E-Safety technical requirements outlined by DGfL, which is aligned to national guidance, *including filtering and monitoring standards.* The managed service provides a number of tools to schools

including Smoothwall Monitor, RM SafetyNet 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 (S Shepherd) can access activity logs for network users and apply 'rules' to specific group of users.
Any changes to filtering and monitoring databases are considered, to ensure there is no unreasonable impact on teaching and learning.

CC4 Access and similar products, are applications that enable a user to remotely access documents and applications stored on the school server. The 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/academy representatives to develop and update a range of Acceptable Use Agreements/guidance *(see Appendix 3)* and include relevant Local Authority Online safety/E-Safety policies and guidance.

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

Teaching and Support Staff:

Are responsible for ensuring that:
- They have an up-to-date awareness of Online safety/E-Safety matters and of the current school/academy Online safety/E-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 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/academy Staff Acceptable Use Agreements (AUA's)
- Head teacher for investigation / action / sanction
- Digital communications with pupils (email / Video conferencing/Virtual Learning Environment (VLE), applications Apps/Google Apps) should be on a professional level and only carried out using official school systems. This is Google classroom
- Online safety/E-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's Online safety/E-Safety Policy and acceptable use agreements
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of Online safety/E-Safety issues related to the use of mobile phones, cameras, hand-held devices *and any device, (wearables) that has the capability of connecting via 4G/5G,* including their personally owned devices, and that they monitor their use and implement current school/academy policies with regard to the use of these devices in the school/academy or during extended school/academy activities. A loan form is available school owned equipment used by staff (see appendix 4 for a sample to be adapted)
- 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 Online safety/E-Safety in their lessons
- Pupils understand that there are sanctions for inappropriate use of technologies, including child on child abuse, 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, Child Protection Policy

5

- 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:

The named person/s (S Shepherd/Louisa Hill) are trained in Online safety/E-Safety issues *and are aware* of the potential for serious child protection issues to arise

- Sharing of personal data
- Publishing of specific information relating to school-based activities involving pupils, via official school systems such as the school/academy web site, external school/academy calendar, *Twitter (X),* Facebook, You Tube
- Sharing of schools owned devices or personal devices that may be used both within and outside of the school/academy
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying, Child on Child abuse, Sexual Harassment, Initiation/hazing type violence and rituals, Sharing of Nude/Semi-nude images (Sexting), 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).

Online safety/E-Safety Committee/Group:
DHT/DSLs /Governor/ staff will assist the Headteacher with:

- The production / review / monitoring of the school Online safety/E-Safety policy / documents
- The production / review / monitoring of the school's filtering *and monitoring processes*
- mapping and reviewing the online safety / digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting with stakeholders – including parents / carers and the students / pupils about the online safety provision
- Identifying current technology/app trends

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 (year 5/6), and 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, *wearables* 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 the school

- Are responsible for the safe use of school/ owned equipment at home, in accordance with the school AUA, for these devices. A guardianship/loan form is available from the office and is required when school owned equipment is used by pupils at home. (See appendix 4)
- Should understand the importance of adopting good Online/E-Safety practice when using digital technologies out of school and realise that the school's/academy's Online/E-Safety policy covers their actions out of school, if related to the use of an externally available web-based system, provided by the school/academy
- Should understand that the school has a 'duty of care' to all pupils. The misuse of non-school/academy provided systems, out of school hours, will be investigated by the school/academy in line with the behaviour, anti-bullying, child protection and other 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, including when away from school. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and training.

Parents and carers will be responsible for:

- Endorsing (by signature) the Student / Pupil Acceptable Use Agreement (year 5/6)
- Accessing the school website / Google classrooms in accordance with the relevant school Acceptable Use /AUA.
- Promoting good online safety practice by following guidelines on the appropriate use of digital and video images taken at school/ events and their children's devices in 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*

Community Users/ 'Guest Access':

Guest access to the internet in the school will be subject to the same filtering rules as other school users. If the school provides access to school software, they need to ensure that the software is not copied or used inappropriately. There should be no access to pupil or staff data or information unless relevant parties have agreed. The school may wish to check portable storage devices such as memory sticks, external hard drives, before they are attached to the school network.

Policy Statement

Education – pupils

There is a planned and progressive Online safety 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 practices.
Online safety education is provided in the following ways:

- A planned Online safety programme is provided as part of Computing and is regularly revisited (termly) – this includes the use of ICT and new technologies in and outside the school
- Key Online safety messages are reinforced as part of a planned programme
- 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 towards radicalisation, by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Pupils are aware of the Pupil AUA's (year 5/6) and are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside the school/academy
- 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
- Rules for use of ICT systems / internet are posted in all rooms
- 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

The school provides information and awareness to parents and carers through:
- Letters, newsletters, school web site,
- Parents evenings,
- Online/E-Safety sessions for parents/carers
- Curriculum activities

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 - Extended Schools/Wider Community

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

Education & Training – Staff/Volunteers

All staff 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. An audit of the Online safety training needs of all staff is carried out regularly.
- All new staff receive Online safety 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 Online safety and DSLs receives regular updates through attendance at DSL, LA, DSPP, training sessions and meetings 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, INSET days and also displayed on the safeguarding board
- The Online safety and DSLs provides advice / guidance / training as required to individuals

All staff are familiar with the school/academy policy including:

- *Filtering and Monitoring systems and associated escalation procedures*
- 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 other school/academy 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/academy owned devices
- Cyberbullying procedures
- Their role in providing Online safety education for pupils
- The need to keep personal information secure

  Filtering and Monitoring: *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*

All staff are formally updated about Online matters at least once a year.

Training – Governors/Directors

Governors take part in Online safety training and awareness sessions, particularly those who are members of any sub-committee involved Computing, safeguarding and Online Child Protection
.
This is offered by:

- Attendance at training provided by the Local Authority, 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' 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 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 are provided with a username and password
- Users are required to change their password every term
- Users are 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 RM SafetyNet filtering. *Changes to filtering and monitoring databases are ratified by SLT and are auditable and the reason for these changes is recorded. The audit trail is reported to governors*
- The school manages and updates filtering requests through the RM Service desk
- 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 and *DSLs*
- 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 incident 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. This is auditable
- An agreed procedure is in place (included in the acceptable use agreement) regarding the extent of personal use that users (staff / students / pupils / community users) 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 (included in the acceptable use agreement) regarding the use of removable media (e.g. memory sticks, hard drive) 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

Curriculum

Online safety is a focus in all areas of the curriculum. The Computing Curriculum specifically identifies 'Digital Literacy' as a focus. Digital Literacy is taught. Staff will re-enforce Online safety 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/
- The school teaches 'Digital Literacy' as part of the '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, child on child abuse, Sharing of Nude/Semi-nude images (Sexting), Cybercrime and Radicalisation (age dependent) and know how to seek help if they are affected by any form of online bullying or exploitation. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button

Use of digital and video images

When using digital images, staff inform and educate 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. (specify age/SEN status related differences)

- 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/academy 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 https://dudleysafeguarding.org.uk/children/parents-and-carers/online-safety-and-use-of-images/
- Pupil's work can only be published with the permission of the pupil (age appropriate) and parents or carers. Parents/carers should have signed the 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 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

Remote Working: Communicating with parents, carers and pupils

Where education is taking place remotely, it's important for schools, teachers and pupils to maintain professional practice as much as possible.

When communicating online with parents and pupils, staff:

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

Video and online conferencing/lessons:

Recording of video conferences

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

However, where video conferencing is used (MS Teams), the school considers the following safeguarding points:

NB for the purpose of this, the term participant refers to a child, young person or vulnerable adult (delete/add as appropriate)

- Staff members do not hold one-to-one video conferences with a participant due to safeguarding risk. Where a video conference is required with an individual, two members of staff are present on the video conference
- Staff members work against a neutral background. Staff present themselves as they would if they were giving a face-to-face lesson/ meeting, both in dress and in manner
- The school has an agreed etiquette for video conferencing which is understood by stakeholders
- Participants are asked to have a neutral background and present themselves as they would in a face-to-face lesson/tutorial/meeting and dress appropriately e.g. not in their sleep wear or dressing gowns
- Participants are aware that some video conferencing platforms save a copy of all chat and all conversations (one to one and group), even it is deleted afterwards. Anything written down could be asked for in an information access request
- Where lessons/tutorials are delivered to a class, parents/carers and students are provided with safeguarding and etiquette guidance in advance of the lesson/tutorial e.g. the student should participate in a room with an open door and parents/carers should try and ensure a trusted adult is in the same premises as the student while the lesson takes place

- The school may choose to record the lesson/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

- The participant will have the choice to turn their camera on
- Where the lesson/tutorial/meeting is recorded with the participants camera on and thus capturing their image, full written parental / carer consent has been sought. Where consent is not given, the lesson/ tutorial/meeting is not recorded if the participant has their camera/microphone switched on

Recording of a video conference is not permitted for some limited matters. If you have any doubts as to whether your video conference will fall under any of the below categories, you should contact your organisations Designated Safeguarding Lead and Data Protection Officer in the first instance for advice. Call recording is not permitted where the meeting includes discussions about individuals with regards to any of the below. This includes current, former or prospective students, staff or service users:
• Counselling, wellbeing or welfare
• Any disciplinary hearing including those relating to safeguarding

Data Protection

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

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

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 system, 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 a portable computer system:
- 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.
- Personal data must not be stored on UBS sticks or removal hard drives

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 nonstandard or personal email accounts these are not secure and cannot always be monitored)*
- Users are aware that email communications may be monitored
- Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and pupils or parents / carers (email, chat, school/academy 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
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Personal information should not be posted on the school website, on public facing calendars and only official email addresses should be used to identify members of staff
- Mobile phones, smart watches may be brought into the school by pupils in year 6 only and the phones must be handed into the teacher who send them to the office.
- 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 Twitter, Google Classrooms and Teams 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 provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school/academy, 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.

Personal Use:

Personal communications which do not refer to or impact upon the school are outside the scope of this policy

Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

The school permits reasonable and appropriate access to private social media sites

14

Monitoring of Public Social Media:

As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.

The school will effectively respond to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and e-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.
The school will take all reasonable precautions to ensure Online safety is a key focus.
However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school/academy computer or mobile device.

Staff and pupils are given information about unacceptable use and possible sanctions. Sanctions available include:
- Interview by Head teacher.
- Informing parents or carers.
- Counselling
- Removal of Internet or computer access for a period, (which could ultimately prevent access to files held on the system, including examination coursework).
- Referral to LA or external support agencies

School policies include infringements relating to online activities (e.g. Behaviour policy, Anti-bullying policy, Child Protection policy)

Our Online safety Coordinator and DSLs acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with school, DSPP child protection procedures.

Policy was approved by Governors: **4th October 2023**

Date for review: September 2024

Contact: Mrs S Shepherd

This Online safety/E-Safety Guidance and Policy has been written with references to the following sources of information:
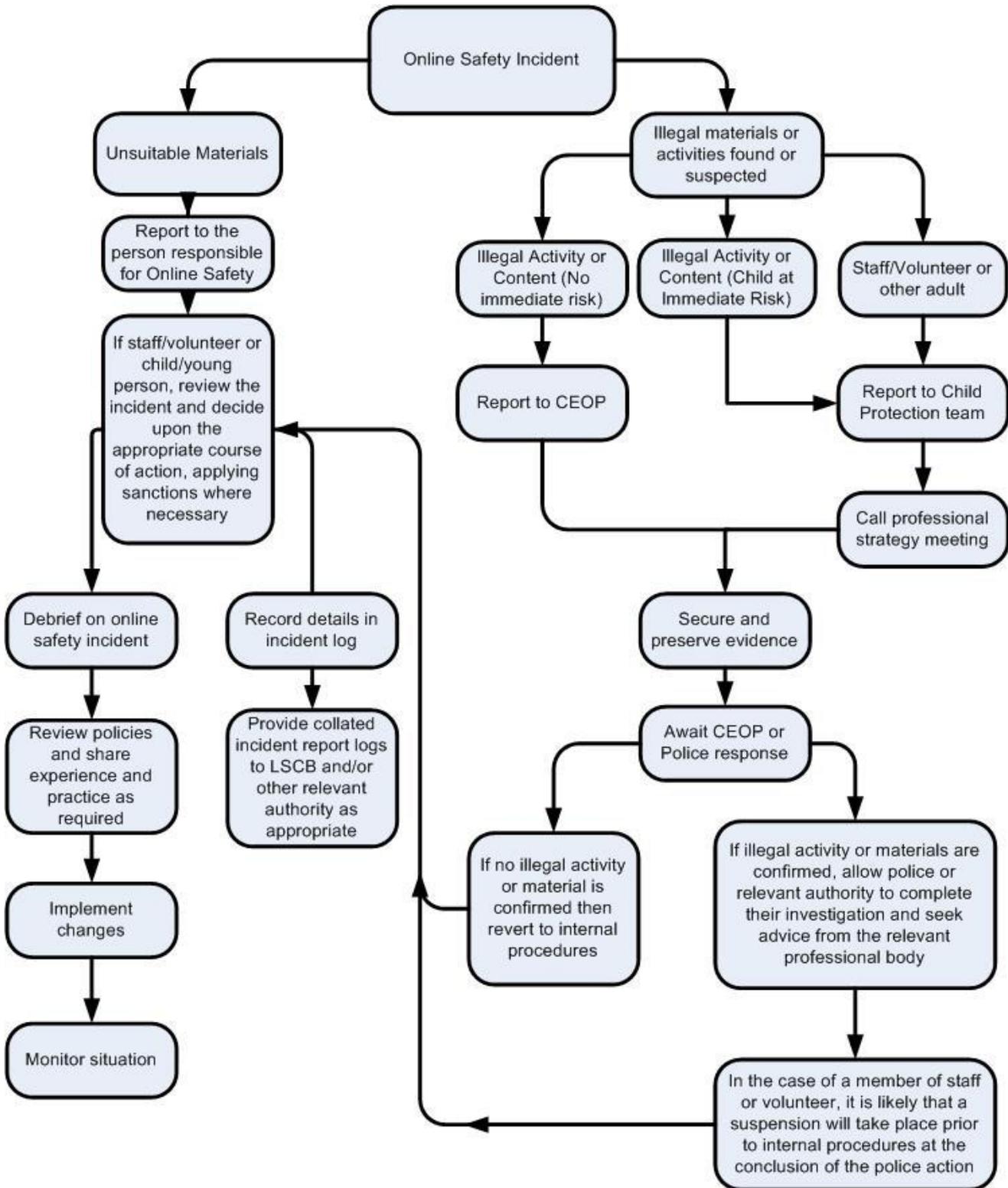Dudley LA
DSPP
Hertfordshire E-Safety Policy
Kent e-Safety Policies, Information and Guidance
South West Grid for Learning- Online Safety School template Policies

Appendix 1 - E-Safety/Online safety sample response

Online Safety Incident

Unsuitable Materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Review policies and share experience and practice as required

Implement changes

Monitor situation

Record details in incident log

Provide collated incident report logs to LSCB and/or other relevant authority as appropriate

Illegal materials or activities found or suspected

Illegal Activity or Content (No immediate risk)

Illegal Activity or Content (Child at Immediate Risk)

Staff/Volunteer or other adult

Report to CEOP

Report to Child Protection team

Call professional strategy meeting

Secure and preserve evidence

Await CEOP or Police response

If no illegal activity or material is confirmed then revert to internal procedures

If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Appendix 2-E-Safety tools available on the DGfL network

E-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

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

- staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- school / academy 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

St Margarets at Hasbury CE Primary School

Rules for Responsible Internet Use

For Primary Pupils

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

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

I agree that:

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

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

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

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

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

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

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

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

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

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

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

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

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

I understand that I am responsible for my actions both inside and outside of school

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

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

Signed:………………………………………………

PRINT NAME…………………………………………

Dated: ………………….

Appendix 3-

St Margarets at Hasbury CE Primary School

Staff Acceptable Use Agreement

Rules for Responsible Internet use

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

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

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

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

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

Official school systems must be used at all times.

Use of school devices (e.g.laptop)
When using a school device either inside or outside school please remember
- it is for work use only
- it is only to be used by yourself, not family members
- no personal data (containing school, pupils etc) should be stored on USB stick or removable hard drive
- to ensure the school device isn't left anywhere unattended

Use of the Internet and Intranet
When entering an internet site, always read and comply with the terms and conditions governing its use. Be aware at all times that when visiting an internet site, the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying your school. For your information, the following activities are criminal offences under the Computer Misuse Act 1990:
- unauthorised access to computer material i.e. hacking;
- unauthorised modification of computer material; and
- unauthorised access with intent to commit/facilitate the commission of further offences.
In line with this policy, the following statements apply: -
- If you download any image, text or material check if it is copyright protected. If it is then following the school procedure for using copyright material.

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

Electronic Mail

Care must be taken when using e-mail as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school.

Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your head teacher. Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the School's business purposes which include the following:

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

In line with this policy the following statements apply: -
- You should agree with recipients that the use of e-mail is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted e-mail is not secure.
- Do not send sensitive personal data via email unless you are using a secure site or portal. It is good practice to indicate that the email is 'Confidential' in the subject line.
- Copies of emails with any attachments sent to or received from parents should be saved in a suitable secure directory.
- Do not impersonate any other person when using e-mail or amend any messages received.
- Sending defamatory, sexist or racist jokes or other unsuitable material via the internet or email system is grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making such comments verbally or in writing.
- It is good practice to re-read e-mail before sending them as external e-mail cannot be retrieved once they have been sent.
- If the email is personal, it is good practice to use the word 'personal' in the subject header and the footer text should indicate if it is a personal email the school does not accept responsibility for any agreement the user may be entering into.
- Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your headteacher.
- All aspects of communication are protected by intellectual property rights which might be infringed by copying. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights.

Social networking

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

School staff may need to request access to social networking sites for a number of reasons including:
- Advertising the school or managing an 'official' school presence,
- For monitoring and viewing activities on other sites
- For communication with specific groups of adult users e.g. a parent group.

Social networking applications include but are not limited to:
- Blogs
- Any online discussion forums, including professional forums
- Collaborative spaces such as Wikipedia
- Media sharing services e.g. YouTube, Flickr
- 'Microblogging' applications e.g. Twitter

When using school approved social networking sites, the following statements apply: -
- School equipment should not be used for any personal social networking use
- Staff must not accept friendships from underage pupils. The legal age for students to register with a social networking site is usually 13 years; be aware that some users may be 13 or younger but have indicated they are older
- It is important to ensure that members of the public and other users know when a social networking application is being used for official school business. Staff must use only their @<schoolname>. dudley.sch.uk email address or other school approved email mechanism and ensure all contributions are professional and uphold the reputation of the school
- Social networking applications should not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- Postings should not be critical or abusive towards the school, staff, pupils or parents or used to place a pupil, student or vulnerable adult at risk of harm
- The social networking site should not be used for the promotion of personal financial interests, commercial ventures or personal campaigns, or in an abusive or hateful way
- Ensure that the appropriate privacy levels are set. Consider the privacy and safety settings available across all aspects of the service – including photos, blog entries and image galleries. Failing to set appropriate privacy levels could result in messages which are defamatory, libellous or obscene appearing on your profile before you have chance to remove them
- It should not breach the schools Information Security policy

Data protection

The processing of personal data is governed by the current Data Protection Act.
As an employee, you should exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of the School. The main advantage of the internet and e-mail is that they provide routes to access and disseminate information.

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

- keep the data private and confidential and you must not disclose information to any other person unless authorised to do so. If in doubt, ask your Head Teacher or line manager;
- familiarise yourself with the provisions of the current Data Protection Act and comply with its provisions;
- familiarise yourself with all appropriate school policies and procedures;

- not make personal or other inappropriate remarks about staff, pupils, parents or colleagues on manual files or computer records. The individuals have the right to see all information the School holds on them subject to any exemptions that may apply.

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

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

Signed:…………………………………………………

PRINT NAME……………………………………………

Dated: ………………….

St Margarets at Hasbury CE Primary School

Community User- Acceptable Use policy

Rules for Responsible Internet use

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

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

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

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

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

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

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

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

Signed:………………………………………………

PRINT NAME……………………………………………

Dated: ……………

St Margarets at Hasbury CE 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 (hard drive, USB flash drives / memory sticks) are checked for viruses before data transfer to the mobile device where appropriate and will not storw any personal data on the;
- 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 …/…/…

St Margarets at Hasbury CE 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 access, download, store or collect any inappropriate material on the device
- I will ensure that all external media sources (hard drive, 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
- 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
- If the equipment is damaged, lost or stolen (no crime reference number given), I will pay for the repairs/replacement

Parents/Carer 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 …/…/…

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