HALES VALLEY TRUST

Online safety Policy

Policy Tracker – Responsibility for monitoring this policy: Online safety officer (Reviewed annually)			
Date of review	**Reviewed By:**	**Role**	**Date Approved by the Governing Board/committee**
22/5/19	Claire Johnson Jeannette Mackinney	Deputy Headteacher, Hurst Hill CEO	June 2019

This document has been produced at the request of Hales Valley Multi-Academy Trust (HVT), with the ideology of ensuring all schools within the trust follow one rigorous and robust online safety (Online safety) policy. The following guidance has been created to support the needs of staff, children and the wider community, so that together we can utilise current technologies safely in the digital world.

It is recognised that new technologies are constantly evolving at a rapid pace and are embraced by users to enhance teaching, learning and as a mode for continuous communication. To reflect this, it is important that Online safety policies are reviewed on an annual basis. As a result, this policy will be reviewed in September 2020.

This policy has been designed to interweave and support other well-being policies, and as such the following policies should also be consulted and revised accordingly: *PSHE policy, Behaviour policy, Anti-bullying policy, Child Protection policy and Safeguarding policy, Social Media and Mobile Phone policy.*

Online Safety/Online safety Advice and Guidance

Rationale

The requirement to ensure that staff, children and young people are able to use the internet and related communication 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 academy community (including all employees, pupils, volunteers, parents / carers, visitors and community users) who have access to and are users of school / academy ICT systems.

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

The 2011 Education Act further 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. This can and may result in using the added power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices if it is deemed inappropriate and potentially harmful to another pupil's well-being. Further information is available in the 'Advice for Headteachers, school staff and governing bodies January 2018 documentation':

School Electronic Devices - Search and Deletion Template Policy

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

Development, Monitoring and Review of the Online safety Policy:

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

- HVT Online safety Coordinators
- Designated Safeguarding Leaders
- Senior Leaders
- Teachers
- Pupils
- ICT Technical Staff
- Governors/Board of Directors
- Parents and Carers
- Community Users

Consultation with the academy community has taken place through the following:

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

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

- Incidents logged on CPOMS
- DGfL or internal monitoring logs of internet activity (including sites visited) via E Safe
- Internal monitoring of data for network activity
- Surveys / questionnaires of stakeholders-including 'pupil voice'
- Updates from the LA
- Attendance at DSL seminars
- LA bulletins/managed service bulletins
- Communications from external agencies
- CEOP Ambassadors

Roles and Responsibilities

Governors/Board of Directors:

Governors and directors within HVT are responsible for the approval of the Online safety policy and for reviewing its effectiveness. This will be carried out annually by the Governors during individual school and academy Governor meetings; through monitoring/audits of Online safety incidents recorded on CPOMS and by keeping up to date with evolving Online safety research and government recommendations. Governors will also ensure that all new staff and pupils have been made aware of the Online safety policy and they have signed the *Acceptable Use Agreements - see Appendix.*

A member of the Governing Body (Kate Davis) who has taken on the role of Safeguarding, will oversee Online safety.

The role of the Online safety Governor will include:

- Meeting with the Online safety Co-ordinator
- Updates on the monitoring of Online safety incident logs and updates on the monitoring of the filtering of web sites/change control logs
- Reporting to relevant Governor/ Boards/ committees / meetings
- Attendance at any Online Safety meetings potentially held within schools, conferences and training as part of the annual Safeguarding CPD updates.

Head teacher and Senior Leaders:

The Head teacher (Rebecca Keen) of each school within HVT is responsible for ensuring the safety (including Online safety) of members of their school and will liaise with the academy community. Each school also has a Senior Information Risk Owner (SIRO). In some cases, this may also be the Head teacher. Each school's SIRO within the academy is responsible for reporting security incidents as outlined in the HVT Information Security Policy.

- All Headteachers have a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Online safety Officer (Deborah Jones).
- HVT Headteachers and (at least) another member of the Senior Leadership Team (Claire Johnson) 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.

  Additional information:
  https://safeguarding.dudley.gov.uk/safeguarding/child/work-with-children-young-people/management-of-allegations/
  http://safeguarding.dudley.gov.uk/report-it/

- Headteachers / Senior Leaders are responsible for ensuring that the Online Online safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- Headteachers / 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 will include annual CPD and allocated timetables for monitoring. Senior leaders will receive regular monitoring reports from the Online safety Co-ordinator. Contents will be shared within SLT/MAT review meetings with the HVT SIRO. This process

is to provide a safety net and support to those colleagues who take on important monitoring roles.

- Head teachers are 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. Each school website provides a link to each school policy relating to Information Security and Data Protection. *https://safeguarding.dudley.gov.uk/safeguarding/adults/work-with-adults/safeguarding-polices-and-procedures/*
- The Head teacher or a designated member of the SLT is responsible for ensuring that parents/carers understand that the school/academy **may** investigate any reported misuse of systems, by pupils, out of school hours, as part of 'safeguarding' procedures as specified in the *Behaviour Policy, Safeguarding Policy and Anti-Bullying policy*

Online safety Coordinator:

Each school within HVT has a named person with the day to day responsibilities for Online safety. This is Deborah Jones at Hurst Hill Primary School.

Responsibilities include:

- Leading an Online safety committee/digital leaders where appropriate
- Taking day to day responsibility for Online safety issues and having a leading role in establishing and reviewing Online safety policies / Online safety documents
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an Online safety incident taking place
- Providing training and advice for staff
- Liaising with the Local Authority/MAT
- Liaising with the academy's SIRO to ensure all school and academy data/information is kept safe and secure
- Liaising with academy ICT technical staff and school/academy contact from the managed service provider- RM
- Receiving reports of Online safety incidents and creating a log of incidents to inform future Online safety developments
- Meeting with the Online safety Governor to discuss current issues, review incident logs and filtering
- Attending relevant meetings / Governor committee meetings
- Cascading centrally communicated updates as appropriate
- Reporting regularly to the Senior Leadership Team

Managed service provider DGfL3:

The managed service provider is responsible for helping each school within the academy to ensure that it meets Online 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 keep users safe -*(see appendix* 2). Schools within HVT 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. Each school nominates 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/academy server/servers. The school/academy has responsibility for ensuring files and applications accessed via this system comply with information and data security practices.

The DGfL Client team currently work with schools within the academy to develop and update a range of Acceptable Use Agreements/guidance *(see Appendix 3)* and provide CPD / advice for Online safety policies and guidance in line with current safeguarding legislation:

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

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

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

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

Teaching and Support Staff:

Are responsible for ensuring that:

- They have an up to date awareness of Online safety matters and of the current academy Online safety policy and practices
- They have read and signed to confirm they have 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 and peers safe
- They have read, understood and signed the academy Staff Acceptable Use Agreements (AUA's)
- They report any suspected misuse or problem to the Online safety Co-ordinator / Head teacher or DSL for investigation
- Digital communications with students (email / Virtual Learning Environment (VLE), applications/O365 Apps/Google Apps / voice) should be on a professional level and only carried out using official school/academy systems
- Online safety issues are embedded in all aspects of the curriculum, in line with the statutory 2014 curriculum requirements
- Pupils understand and follow the academy Online 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/academy activities
- They are aware of Online safety issues related to the use of mobile phones, cameras and hand-held devices, including their personally owned devices and that they monitor their use and implement current academy policies with regard to the use of these devices in the academy or during extended academy activities.
- In lessons, where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable

material that is found in internet searches. They include the teaching of Online safety in their lessons
- Pupils understand that there are sanctions for inappropriate use of technologies and the academy will implement these sanctions in accordance with the Behaviour Policy, Safeguarding policy and Anti Bullying Policy
- Pupils understand that the academy 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 DSL's at Hurst Hill Primary School are Rebecca Keen, Claire Johnson and Joanna Potts, they are trained in Online 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 academy-based activities involving pupils, via official academy systems such as the school or academy web site, external school/academy calendar, Twitter or Facebook.
- Sharing of school/academy 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, Radicalisation, CSE

Pupils:

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

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Agreement/ Acceptable Use Agreement (AUA) *(see appendix 3*), which they, and their carers will be expected to sign before being given access to school systems (found in pupil planners)
- 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 and academy policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand academy 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 multi academy trust.
- Are responsible for the safe use of school owned equipment at home, in accordance with the school/academy (AUA), for these devices. Should understand the importance of adopting good Online safety practice when using digital technologies out of school and realise that the school's Online safety policy covers their actions out of school, if related to the use of an externally available web-based system, provided by the school/academy

- Should understand that the school has a 'duty of care' to all pupils. The misuse of non-school provided systems, out of school hours, will be investigated by the school in line with the behaviour, anti-bullying 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. Hales Valley Trust will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Learning Platform and information about national / local Online safety incentives and literature

Parents and carers will be responsible for:

- Endorsing (by signature) the Student / Pupil Acceptable Use Agreement
- Accessing the school website / School Learning Platform 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 and at academy events.
- Ensuring that cameras on their mobile phones are not used on the school premises during meetings and when dropping off and collecting the children from school.
- Only taking photographs of their child when visiting school to celebrate events/achievements where the Headteacher has granted permission (*also see 'Use of digital and video images' section*)

Community Users/ 'Guest Access':

Community Users who access school/academy ICT systems / website / School/Academy Learning Platform/on-line student/pupil records or other school/academy provided system as part of the Extended School provision, will be expected to read all Online safety, Safeguarding and Behaviour policies; sign a confidentiality agreement and an acceptable use agreement before being provided with access to academy systems. Schools within the academy trust must ensure that user restrictions are in place to safe guard pupils and staff considering carefully what they are prepared to provide community access to.

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

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

Policy Statement

Education – pupils

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

- A planned Online safety programme is provided as part of Computing / PHSE / RSE lessons and is regularly revisited – this includes the use of ICT and new technologies in and outside the school/academy
- Key Online safety messages are reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils are taught in all lessons to be critically aware of the 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 to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Pupils are educated about the dangers of sexting during Upper Key Stage Two RSE lessons
- Pupils are aware of the Pupil AUA's and are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside the 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 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 authorised the Head or Deputy Head Teacher and be auditable
- Rules for use of ICT systems / internet are posted in class rooms and are displayed on log-on screens and in homework planners. Is this relevant to all? (SMART)
- Pupils are taught the importance of information security and the need to keep information such as their password safe and secure
- Staff act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

Schools within Hales Valley Trust provide information and awareness of online safety to parents and carers through:

- Letters, newsletters, school web sites, and the school learning platform.
- Parents evenings, Reception/Year induction meetings
- Online/Online safety sessions for parents/carers where appropriate
- High profile events or campaigns such as Safer Internet Week
- Family learning opportunities
- Curriculum activity maps

Education - Extended Schools/Wider Community

The school/academy offers family support in Online Safety/Online safety so that parents/carers and children can together gain a better understanding of these issues.
Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education & Training – Staff/Volunteers

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

- Annually, 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 a quality safeguarding induction inclusive of Online safety training, ensuring that they fully understand the academy Online safety Policy and Acceptable Use Agreements
- The Online safety Coordinator and school DSL receives regular updates through attendance at DSL/DGfL / LA training sessions and by reviewing guidance documents released by DfE / DGfL / LA, DSCB and others
- This Online safety policy and its updates are presented to and discussed by staff in staff / team meetings and annually during INSET.
- The Online safety Coordinator and DSLs provide advice / guidance and training as required to additional individuals

All staff are familiar with the academy 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/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/academy website
- Capturing and storing photographs/videos/audio files on personal and school/academy owned devices
- Cyberbullying procedures
- Their role in providing Online safety education for pupils
- The need to keep personal information secure

All staff are formally updated about Online safety matters at least once a year during their annual Safeguarding CPD

Training – Governors

Governors are invited to take part in Online safety training sessions, particularly those who are members of any sub-committee: Health and Safety / Child Protection

.

This is offered through:

- Attendance at training provided by the Local Authority / National Governors Association / DGfL/ LSCB or other relevant organisation

- Participation in school/academy 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. Each HVT school is responsible for ensuring that policies and procedures approved within this document are implemented.

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

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

School and Academy ICT systems will be managed in ways that ensure that the school/academy meets the Online/Online safety technical requirements.

- There will be regular reviews and audits of the safety and security of school/academy 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 and academy ICT systems

- All users will be provided with a username and password (Foundation and year one pupils will be provided with a suitable generic password and additional restrictions put in place to monitor the AUA)
- Users will be required to change their password every three months. Each HVT school has implemented the 'DGfL Security Enhancements' which include a policy to force users to change their password regularly and can define the level/complexity of password required
- Users will be made responsible for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- Each school within the academy maintains and supports the managed filtering service provided by DGfL. The academy can provide enhanced user-level filtering through the use of Smoothwall filtering or a MDMs (Managed Mobile Device system)
- The school/academy manages and updates filtering requests through the RM Service desk
- Requests from staff for sites to be removed from the filtered list must first be considered by the Head Teacher and put in writing. If the request is agreed, this action will be recorded, and logs of such actions shall be reviewed regularly by the Online safety Committee
- An appropriate system is in place for users to report any actual / potential Online safety incident to the relevant person
- The managed service provider ensures that appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices

etc from accidental or malicious attempts which might threaten the security of the school/academy 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/academy system. This is auditable
- A guardianship document is signed before school/academy 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/academy workstations / portable devices
- The school/academy 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
- Each school within the academy has responsibility for ensuring files and applications accessed via CC4 Access or a similar application, comply with information and data security practices.

Curriculum

Online safety is a focus in all areas of the curriculum. The new 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 and RSE 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
- Each school provides opportunities within a range of curriculum areas to teach about Online safety
- The schools teach ‘Digital Literacy’ as part of the new ‘Computing’ programme of study
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the network manager or managed service provider temporarily remove those sites from the filtered list for the period of study. Any requests to do so are auditable and should be logged
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils will be educated and made aware of the impact of Cyberbullying, Sexting and Radicalisation. They will 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 Child.net/ NSPCC or the CEOP report abuse button.

Use of digital and video images

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

- Staff can take digital / video images to support educational aims, and follow school and academy policies concerning the storing, sharing, distribution and publication of those images. Those images are only taken on school or academy equipment, the personal equipment of staff is not used for such purposes
- Pupils are not permitted to use personal digital equipment, including mobile phones, smart watches and cameras, to record images of the others, this includes when on field trips. However, with the express permission of the Head teacher, images can be taken provided they are transferred immediately and solely to the school's or academy's network and deleted from the pupil's device.
- Care is taken when capturing digital / video images, ensuring students / pupils are appropriately dressed and that they are not participating in activities that might bring the individuals or the school or 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, newsletter or blog, particularly in association with photographs
- Written permission from parents or carers is obtained before photographs of pupils are published on the school or academy website, or on an official school/academy social networking application as in line with the Dudley Safeguarding Children's Board-DSCB consent form
  DSCB Guidance/Policies:
  https://safeguarding.dudley.gov.uk/safeguarding/child/work-with-children-young-people/Online safety-and-use-of-images/
- Pupil's work can only be published with the permission of the parents or carers. Parents/carers should have signed the DSCB consent form
- In accordance with guidance from the Information Commissioner's Office, at the Head Teacher's discretion, parents / carers may be given permission to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images. Where the Headteacher of the school does grant permission, parents/carers with be asked to sign a declaration upon arrival to the event. Please note that children with certain vulnerabilities may prevent photographs being taken at events.

Data Protection

Hales Valley Multi Academy Trust has a Data Protection Policy that meets statutory guidance.

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

- *It has 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).*
- *It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for*

- *Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay*
- *The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice*
- *Where special category data is processed, a lawful basis and a separate condition for processing have been identified*
- *Data Protection Impact Assessments (DPIA) are carried out*
- *It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers*
- *Procedures are in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller*
- *There are clear and understood data retention policies and routines for the deletion and disposal of data*
- *There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible*
- *Consideration has been given to the protection of personal data when accessed using any remote access solutions*
- *The Freedom of Information Policy sets out how FOI requests are actioned*

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

- Take care at all times, to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Access personal data on secure password protected computers and other devices, at the school/academy and home, or via the school Learning Platform, 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/academy policy once it has been transferred or its use is complete.

Please refer to guidance available from Dudley Information Governance:

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

Communications

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

- The official school and academy email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school/academy email service to

communicate with others when in the school, or on school systems e.g. by remote access from home

- Users are aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the academy 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) academy 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 and in some cases academy email addresses for educational use.
- Pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They will 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 or academy website, on public facing calendars and only official email addresses should be used to identify members of staff
- Smart watches may not be brought into school by pupils
- Year 6 pupils are allowed to bring personal mobile devices/phones into school. However, they must not be used in lesson time and we therefore request for such devices to be handed into reception at the beginning of the day and collected at home time. Parents are asked to complete a permission slip in order for this happen.
- The academy allows staff to bring in personal mobile phones and devices for their own use. However, mobile phones may only be used in designated areas within school and only in the absence of pupils e.g. – the school staff room or a school office. Mobile phones are prohibited from use in the classroom.
- Under no circumstances should a member of staff contact a pupil or carer using their personal device unless authorised to do so by their Head Teacher.
- 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 academy must ensure there is no inappropriate or illegal content on the device
- The academy provides a safe and secure way of using chat rooms, blogs and other 'social networking technologies' via a Learning Platform or similar system
  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

Commented [MJM1]: I think this is referring to the smart watch rather than the phone. Prob needs to be clearer…

Commented [MJM2]: Would this bullet point cover the one above so we could remove that one?

Social Media - Protecting Professional Identity

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

The schools provide the following measures to ensure reasonable steps are in place to minimise the risk of harm to pupils, staff the school and 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/Academy staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school/academy staff
- They do not engage in online discussion on personal matters relating to members of the school/academy community
- Personal opinions should not be attributed to the school MAT 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 academy permits reasonable and appropriate access to private social media sites.

Monitoring of Public Social Media:

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

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

The school's / academy's use of social media for professional purposes will be checked regularly by the senior leaders within each school to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

All monitoring, surveillance or investigative activities are conducted by authorised staff.
The schools within the academy 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/counselling by class teacher, Online 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, including homework).
- Referral to LA or external support agencies such as social workers or the police in extreme cases of bullying or harassment.

Additional academy policies include infringements relating to online activities: Behaviour policy, Anti-bullying policy, Child Protection policy, Staff Conduct policy

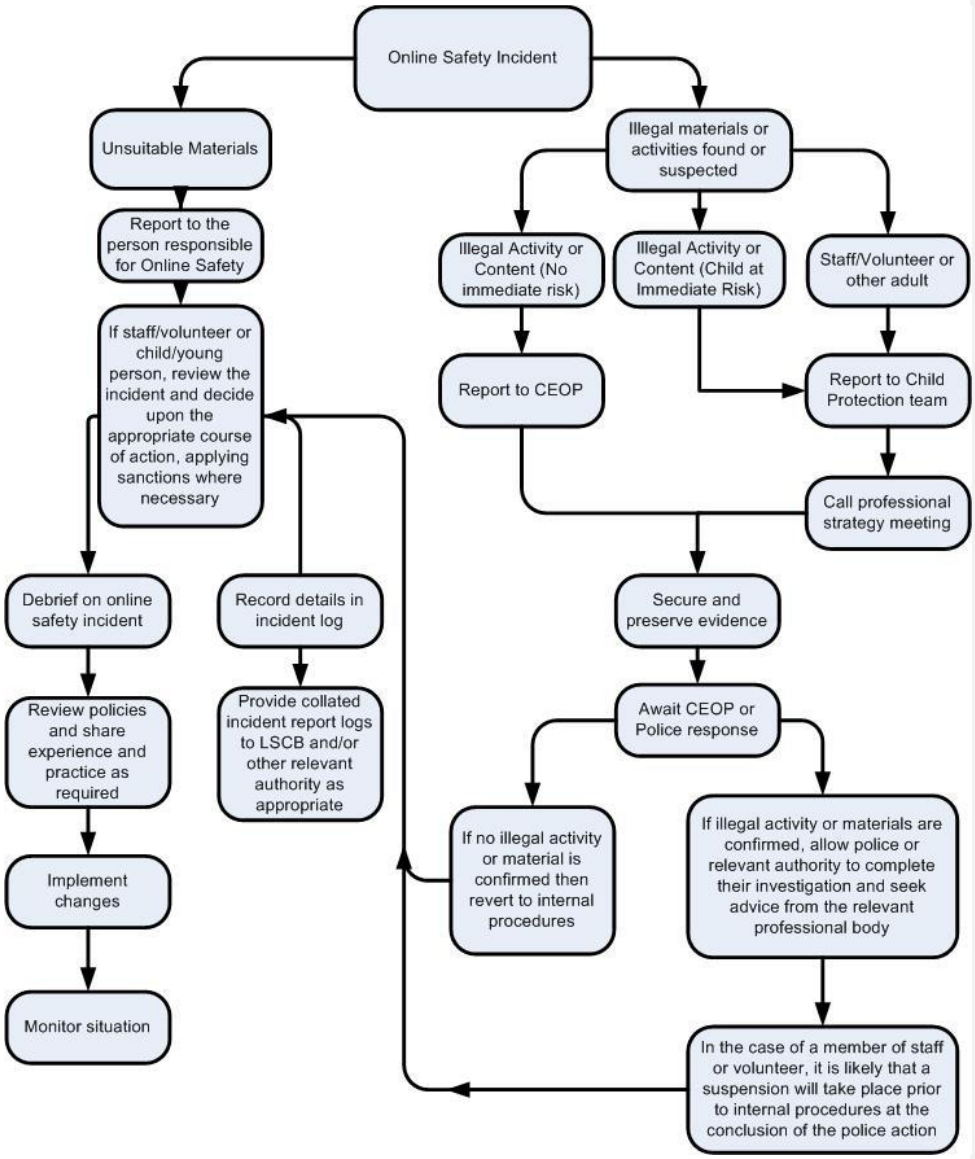
Online safety Coordinator and DSL act as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- 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 /academy, LSCB child protection procedures.

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

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

Appendix 1- Online safety/Online safety sample response



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

Online 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
CC4 AUA	Awareness raising	Part of CC4-needs to be enabled	All CC4 stations at log in	When enabled through the management console, users are given an acceptable use policy at log in
eSafe	Monitoring software-*licenses available on Windows, Apple Mac*	Available to all schools	All school desktops and networked laptops, Chrome books and Apple Mac networks	Takes a snapshot of a screen when an event is triggered. A range of events can be monitored. Reports are sent to designated staff in school
Email	Filtering and list control	Provided as part of DGfL	Office 365	Allows schools to restrict where email is sent from/to
DGfL 'Security Enhancements'	Safe practice	Provided as part of DGfL3	All CC4 stations	A password management policy that enforces password rules of complexity and length for different users

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

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

Pupil Acceptable Use Agreements are intended to ensure that:

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

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

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

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

Community Users Acceptable Use Agreements are intended to ensure that:

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

Appendix 3- Example Primary pupil AUA

Hales Valley Trust- Lapal Primary School

Rules for Responsible Internet Use

For Primary Pupils

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

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

I agree that:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Signed:……

PRINT NAME……

Dated: ……..

Appendix 3- Example Staff AUA

Hales Valley Trust

Staff Acceptable Use Agreement

Rules for Responsible Internet use

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

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

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

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

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

Official school systems must be used at all times.

Use of the Internet and Intranet

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

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

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

- If you download any image, text or material check if it is copyright protected. If it is then follow the school procedure for using copyright material.
- Do not download any image, text or material which is inappropriate or likely to cause offence. If this happens accidentally report it to a senior member of staff.
- If you want to download any software, first seek permission from the Head Teacher and/or member of staff responsible /RM. They should check that the source is safe and appropriately licensed.

- If you are involved in creating, amending or deleting web pages or content on the web site, such actions should be consistent with your responsibilities and be in the best interests of the School.
- You should not:
    - introduce packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;
    - seek to gain access to restricted areas of the network;
    - knowingly seek to access data which you are not authorised to view;
    - introduce any form of computer viruses;
    - carry out other hacking activities.

Electronic Mail

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

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

In line with this policy the following statements apply: -

- You should agree with recipients that the use of e-mail is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted e-mail is not secure.
- Do not send sensitive personal data via email unless you are using a secure site or portal. It is good practice to indicate that the email is 'Confidential' in the subject line.
- Copies of emails with any attachments sent to or received from parents should be saved in a suitable secure directory.
- Do not impersonate any other person when using e-mail or amend any messages received.
- Sending defamatory, sexist or racist jokes or other unsuitable material via the internet or email system is grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making such comments verbally or in writing.
- It is good practice to re-read e-mail before sending them as external e-mail cannot be retrieved once they have been sent.
- If the email is personal, it is good practice to use the word 'personal' in the subject header and the footer text should indicate if it is a personal email the school does not accept responsibility for any agreement the user may be entering into.
- Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your 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 Data Protection Act 1998. Schools are defined in law as separate legal entities for the purposes of complying with the Data Protection Act. Therefore, it is the responsibility of the School, and not the Local Authority, to ensure that compliance is achieved.
As an employee, you should exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of the School. The main advantage of the internet and e-mail is that they provide routes to access and disseminate information.

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

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

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

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

Signed:……

PRINT NAME……

Dated: ……..

Hales Valley Trust

Community User- Acceptable Use policy

Rules for Responsible Internet use

This policy applies to all community users of the school's systems, who have guest access to the internet. We trust you to use the ICT facilities sensibly, professionally, lawfully, and in accordance with this Policy.
It is important that you read this policy carefully. If there is anything that you do not understand, please ask. Once you have read and understood this policy thoroughly, you should sign this document, retain a copy for your own records and return the original to the school office.
Research Machines (RM) has a contractual obligation to monitor the use of the internet and e-mail services provided as part of DGfL, in line with The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Traffic data and usage information may be recorded and RM, Dudley MBC and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request.

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

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

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

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

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

Signed:……

PRINT NAME……

Dated: ……

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

<School Name >

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)

<School Name >

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 …/…/…