Wilkinson Primary School

Online Safety (e-safety) Policy

Date: October 2025 - 26

Contents

Development/ Monitoring/ Review of this Policy

This Online Safety policy has been developed by a working group consisting of:

- Headteacher and Senior Leaders
- Online Safety Coordinator
- DSL/DDSL
- Staff – including Teachers, Support Staff, Technical staff
- Governors

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This Online Safety policy was implemented on:	September 2025
This Online Safety policy was approved by the Governing Body on:	October 2025
The implementation of this Online Safety policy will be monitored by the:	Governing Body Senior Leadership Team
Monitoring will take place at regular intervals:	Annually
Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Annually
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2026
Should serious online safety incidents take place, the following persons / agencies should be informed:	Headteacher, DSL/DDSL, LA Safeguarding Officer, LADO, Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - pupils
    - parents / carers
    - staff

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital technology 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 online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school but is 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 can only be taken over issues covered by the published Behaviour Policy.

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

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

Governing Body

The Governing Body is responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing Body receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to Governing Body meetings

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Coordinator.
- The Headteacher and (at least) another member of the Senior Leadership Team will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included below – "Responding to incidents of misuse" and relevant Local Authority disciplinary procedures).
- The Headteacher is responsible for ensuring that the 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 necessary.
- The Headteacher and 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 also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Coordinator.

Online Safety Coordinator

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- ensures, with the school's technical support, that the school has robust and up-to-date monitoring and filtering software (the school uses SENSO as its monitoring software)
- receives and examines online safety incident logs generated by the school's monitoring software, deciding on what actions need to be taken for each incident whether this is categorising as a false positive or investigating incidents.
- Investigates any incidents described as critical or urgent by the school's monitoring software and liaising with SMT as to what action, if any needs to be taken
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to Senior Leadership Team
- implements an effective scheme of work for digital safety/digital citizenship
- maintains an up-to-date policy on Remote (Home) Learning including measures and procedures to keep children safe whilst working remotely.

Technical Support

Technical Support is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Learning Platform / email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher / Senior Leaders ; Online Safety Coordinator for investigation / action / sanction.
- that monitoring software / systems are implemented and updated as agreed in school policies – the school uses SENSO as it's monitoring system.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Headteacher / Senior Leader / Online Safety Coordinator / DSL/DDSL for investigation / action / sanction
- there is no digital communications with pupils, parents/carers (any digital communication with parents/carers should only be carried out by office staff, will be on a professional level and only carried out using official school systems). There is no reason whatsoever why a member of the teaching staff (teachers or teaching assistants) should be using digital means to contact pupils or their parents/carers.
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- Implement the teaching of the digital safety/digital citizenship scheme
- pupils have a good understanding of research skills and the need to uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- 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
- implement the measures and procedures set out in the Remote (Home) Learning to keep children safe whilst working remotely.

Designated Safeguarding Lead / Deputy Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety Group will assist the Online Safety coordinator with:

- the production / review / monitoring of the school Online Safety Policy / documents.
- the production / review / monitoring of the school Remote Learning Policy / documents.
- mapping and reviewing the online safety and digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet incident logs
- consulting stakeholders – including parents/carers and the pupils about the online safety provision

Students / Pupils

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- 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 their membership of the school
- follow the measures and procedures set out in the Remote (Home) Learning Policy to keep themselves safe whilst working remotely.

Parents / Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' workshops, newsletters, letters and the school's website with information about national/local online safety campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / and any online resource used by the school / online pupil records

- following the measures and procedures set out in the Remote (Home) Learning Policy to keep their children safe whilst working remotely.

Community Users

Community Users who access school systems/website/Office 365 (Teams)/Google Classroom as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education - Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety and digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety will be a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum will be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided as part of Computing/PHRSE curricula
- Key online safety messages will be reinforced as part of a planned programme
- Pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils will be 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. (N.b. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet).
- Pupils should be helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that 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.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in websites being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be made to the Online Safety Coordinator, in writing, with clear educational reasons and a list of the websites to be used and the date(s) and time(s) that access to these websites is required. If such a request is accepted the Online Safety Coordinator will arrange for the filtering to be removed.

Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents' Workshops
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

The school may provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school / academy website will provide online safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online Safety provision

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced and will include biannual whole staff online safety training, yearly update and training for all staff new to the school.
- An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- The Online Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.

Training - Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are involved in technology / online safety / health and safety /safeguarding.

Technical – Infrastructure / equipment, filtering and monitoring & Cybersecurity

The school has technical support provided by Engagedu, the school's broadband connection is maintained by Wolverhampton Council. It is the responsibility of the school to ensure that service providers carry out all the online safety measures that would otherwise be the responsibility of the school, as suggested below. The school will also check the service providers' policies on these technical issues.

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the school's Network Manager. Users are responsible for the security of their username and password.
- The "administrator" passwords for the school ICT systems, used by the Network Manager will be available to the head of the school's technical support service (must also be available to the Headteacher / Principal or other nominated senior leader and kept in a secure place (eg school safe)
- The school's technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of

software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs).

- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider maintained by the school's technical support provider. (by actively employing the Internet Watch Foundation CAIC list). Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Monitoring of the activity of users on the school technical systems is carried out by:
    - A remote monitoring system (Senso), which will:
        - Monitor activity on all devices in use in school (Staff and Pupil, iPad, Laptop and PC), including e-mails
        - Deliver immediate reports of possible issues to the Digital Safeguarding Lead and the Designated Safeguarding Lead
        - Deliver a weekly summary of issues to the Digital Safeguarding Lead and the Designated Safeguarding Lead
        - Maintain a list of issues which can be viewed by to the Digital Safeguarding Lead and the Designated Safeguarding Lead
        - Connect immediately, with the school's Safeguarding recording system (CPOMS) allowing the Digital Safeguarding Lead and The Designated Safeguarding Lead to view incidents, record investigations and follow-up actions

  users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users and their family members are allowed on school devices that may be used out of school.
    - Personal use of school provided devices is allowed for
        - web browsing
        - the use of the provided software/apps available on the device.
    - Personal use of school provided devices does not extend to
        - the storage of personal files (including personal documents, photographs, music and videos).
        - The playing of online games
        - Downloading software or apps for personal use
    - Family members should not use school provided devices
- Staff MUST NOT download executable files and install programmes/apps on school devices.

- Removable media (e.g. memory sticks / CDs / DVDs / External Hard Drives / SD or other Memory Cards) MUST NOT BE USED by users on school devices. The only exception to this is the use of a SD card (or similar) from a digital camera to transfer images from the camera to the hard drive of a computer.
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's Learning Platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, Remote Learning Policy and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

The school Acceptable Use Agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies

The school allows:

	School Devices		Personal Devices		
	School owned for single user	**School owned for multiple users**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*No*	*Yes**	*Yes**
Full network access	*Yes*	*Yes*		*No*	*No*
Internet only				*No*	*No*

* For full details of staff usage of personal devices see policy below.

School owned / provided devices: This refers to devices provided to an individual member of staff for use in the course of their professional duties. It does not refer to devices provided to the pupils for use in the course of their education.

- All staff will be allocated a laptop - one iPad will be allocated to each class.
- Staff may use their devices both in and out of school in the course of their professional duties.
- Personal use is limited (see above). Staff should not store personal files on their devices (including, but not restricted to videos, music, audio files and photographs) on their devices. Staff should not download or install apps/programmes/software for personal use onto their devices. To download a particular app/programme please see the school's technician. However it is recognised that staff may wish to use, for example, particular pieces of music or photographs with their class, in these cases it is permissible for staff to store such files on their school provided laptops as long as they comply with all legal requirements (e.g. only films classified as U may be shown to children).
- All provided devices will have full access to the school's networks and the internet whilst in school. Staff may connect their devices to home networks and the internet outside of school being aware of the restrictions placed upon them regarding the nature and content of any websites they may visit.
- Staff are **solely** responsible for any content found on school provided devices or websites visited.
- Staff should not change any of the settings on their devices other than those that affect the appearance (e.g. home screen/lock screen) of their devices. If staff wish to download apps/programmes or software, they should discuss this with the e-safety coordinator and the technician before doing so.
- Technical support for these devices will be provided by the school's technician. Staff should consult the Computing Coordinator or the technician if they are experiencing difficulties with their device or wish to make changes to any of the settings or download apps/programmes/software.
- Devices are filtered in school from any illegal/damaging content using the local authority's filtering systems. Such filtering will not be available outside of the school. Staff should be aware of this and take all necessary steps to avoid contact with any material that might be considered illegal or damaging.
- There should be, in normal circumstances, no need for staff to access personal cloud based services or storage. However the school recognises that, at times, accessing such services to share video, audio or photographic material as part of the educational experiences they are providing for their children may be necessary. In such cases access to cloud based services is acceptable, but staff should consult the Online Safety Coordinator prior to doing so. Some cloud based services may be blocked by the school's filtering systems. If staff wish to access such services they should discuss this with the e-safety coordinator or head teacher who will contact the technician to have the services unblocked for a specified period of time.

  N.B. under no circumstances should children be allowed to access blocked services.

  N.B. staff will be provided with access to YouTube
- All laptops have a password protected log on and a password protected boot (Bitlocker) that will stop any unauthorised access to the hard drive.
    - Under no circumstances should staff reveal their passwords.

- Staff should not write their passwords or Bitlocker codes down on anything attached to their machines, or on/in anything transported or stored with their device (e.g. in a diary that is transported with the device).
- Staff should be aware that any data on their devices has to comply with the regulations of the GDPR.
- Staff should set strong passwords (advice on setting strong passwords can be provided by the Online Safety Coordinator).

- Staff may use their school provided devices to capture images and store images (still or video) of the pupils of the school if:
  - There is a good educational reason for doing so
  - To record an activity for which no formal written recording takes place
  - To record a memorable event
  - Permission has been granted by the parents for images to be taken of their child (there are several categories to this permission and staff should consult their class records to see what level of photographic permission has been granted).
  - Photographs MUST NOT be taken in the 'pop-up' swimming pool unless specific permission has been given to record swimming lessons for assessment purposes. Such images MUST ONLY be of children IN the pool and every care MUST be taken to ensure ONLY the head and shoulders are plainly visible. UNDER NO CIRCUMSTANCES should pictures be taken of children in swimming costumes when they are not in the pool. Additionally, pictures should not be taken of children whilst they are changing clothes (for any reason, PE, Swimming, school performances etc)

    N.B. cameras and mobile devices are not permitted at the swimming baths
  - School provided devices are used to capture the images
- Images (still or video) of pupils from the school must not, under any circumstances, be transferred to any personal device, be uploaded to the internet or shared on any form of social networking platform.
- Staff MUST NOT use personal devices to take or store images of children (except under the circumstances described below)

  Images (still or video) may be taken in or out of school on school activities (e.g. trip, residential, sporting event)

- If a staff member leaves the school's employment their devices must be returned to the computing coordinator who will pass them to the technician who will wipe the devices and reset them for future use.
- Liability for damage: All devices are insured for accidental damage (e.g. cracked screens). However staff take reasonable steps to ensure their devices are kept and used in a way that does not lead to loss or damage (e.g. awareness of proximity of liquids, sources of heat etc). Devices are only insured for travel in a staff members car if they are locked, out of sight in the boot of the vehicle
- Staff training will be provided on both an ad hoc and formal basis, particularly after updates to vital software (e.g. operating systems).

Personal Devices:

- Staff are allowed to bring their own devices into school, under certain restrictions.
    - Mobile phones must not be used, or be visible, in any area where children are present.
    - The use of a mobile phone is restricted to lunchtimes, before the arrival of children and after their departure and should only be used in the staffroom, or other area away from the children.
    - Children are not allowed, under any circumstances, to use a staff member's personal device.
- Personal devices should be stored securely in a lockable place, preferably the lockers provided in the staffroom. Staff should not keep personal devices in teachers' desks, classroom cupboards or in bags.
- Staff should not use their own devices for school business (except phone calls – see below). However, it is recognised that there may be occasions where a staff member will need to use their own device. This could be if a battery has run out on a school device (though every effort must be made to source an alternative school device – possibly by borrowing from another member of staff) or if vital software is only available on a staff member's personal device (for example Adobe Photoshop). In such cases if a personal device is used, then this use must be logged with the Online Safety coordinator, who will record the circumstances and nature of the use and require a date by which any images, audio or video files is to be removed* (see 'right to examine users devices' and 'Data protection', below). *Removed can include transferred to a school device.
- Staff should not use their personal devices to bypass the schools filtering systems and access the internet without the restrictions of the filtering systems.
- Personal devices will not be allowed to join the school's network, under any circumstances.
- No technical support for personal devices is available
- Data Protection: Staff must not, under any circumstances store pupil or staff data on their own devices (this includes but is not limited to, names, contact details, dates of birth, educational performance data or home circumstances data). Any such storage can be considered as a data breach under the regulations of the GDPR. Storage of pupil images (still or video) is not permitted on personal devices except under the exceptional circumstances described above, with the knowledge of the Online Safety Coordinator (logged) and a date by which these images are to be removed.
- The School reserves the right to take, examine and search user's devices in the case of potential misuse. N.B. this is also included in the Behaviour Policy and Whistle-Blowing Policy.
- The School takes no responsibility or accepts any liability for the loss, damage or malfunction of user's personal devices whilst on school premises, on school business elsewhere or in travelling to or from the school site or any other location on school business.
- Visitors will be informed about school requirements through the normal visitor's information. Visitors will be informed that mobile devices should not be used or be visible around school. If they need to use such a device occurs they should inform the accompanying member of staff/ visit organiser, who will make the necessary arrangements under the procedures described above.
- Education about the safe and responsible use of mobile devices is included in the school Online Safety education programmes.
- Phone calls – use of personal devices; this is permitted when calling school to confirm arrival departure on trips and for booking visits/visitors; though it is recommended that a school telephone is used within school and during school hours.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act/GDPR) if permission is given at the start of the event by a senior leader (who will have checked permissions). To respect everyone's privacy, and in some cases for child protection, parents will be informed that these images should not be published or made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow the school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes (see above).
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Photographs MUST NOT be taken in the 'pop-up' swimming pool unless specific permission has been given to record swimming lessons for assessment purposes. Such images MUST ONLY be of children IN the pool and every care MUST be taken to ensure ONLY the head and shoulders are plainly visible. UNDER NO CIRCUMSTANCES should pictures be taken of children in swimming costumes when they are not in the pool. Additionally pictures should not be taken of children whilst they are changing clothes (for any reason, PE, Swimming, school performances etc) *see above
- 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 will comply with good practice guidance on the use of such images.
- Only pupils' forenames will be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and their parents or carers.

Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR).

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school ensures that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO).
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness/data protection training and are made aware of their responsibilities.

Staff must ensure that they do not use devices that are not encrypted for the storage/transfer of data. They must:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, 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:

- The data must be encrypted and password protected.
- The hard disk of the device must be password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff should not use removable storage devices in school (memory sticks, CD, DVD, External Hard Drives SD or CF cards)*see above for clarification on SD/CF cards from digital cameras.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	✓							✓
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Use of removable storage devices				✓				✓
Taking photos on mobile phone				✓				✓
Taking photos on school cameras/tablets	✓						✓	
Use of other mobile devices e.g. gaming devices				✓				✓

Use of personal email addresses in school, on school network as username on online resources				✓				✓
Use of school /email for personal emails				✓				✓
Use of messaging apps		✓[2]						✓
Use of social media		✓[2]						✓
Use of blogs		✓[1]					✓[1]	

1. Children and staff are allowed to access blogs if they are school created or specifically aimed at primary aged children in the course of their education. For staff use of other blogs see note 2, below.
2. 'Certain Times' for the use of messaging apps, social media and blogs means before children arrive at school, at lunchtime in the staffroom and after the children have left school. Such use should also be only on personal devices.

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. Users should be aware that email communications are monitored. Staff should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, To the Online Safety Coordinator or the DSL/DDSL, Headteacher (Chair of Governing Body if the Headteacher is involved), the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- There should be no digital communication between staff and parents/carers. Email, text etc must be sent via the school office and will be professional in tone and content. These communications may only take place on official (monitored) systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class/group email addresses may be used at KS1, while pupils at KS2 will be provided with individual school email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media – Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, gender orientation, sexual orientation, race or disability or who defame a third party may render the school, and themselves, liable to the injured party.

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

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff MUST ensure that:

- No reference should be made in social media to pupils, or their parents/carers.
- No comments are made about the school, its staff or governors which are likely to cause offence or bring the school, its staff and governors into disrepute.
- 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

Staff MUST be aware that breaching the acceptable use agreement or the conditions stated above will result in disciplinary action, which can involve the Local Authority and may result in disciplinary action including suspension (see table below).

Staff MUST be aware that they are **solely** responsible for any material that appears on their social media accounts/e-mails/texts regardless of how they were caused.

When official school social media accounts are established there will be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
    - Systems for reporting and dealing with abuse and misuse
    - Understanding of how incidents may be dealt with under school / academy disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- No reference should be made in social media to pupils, or their parents/carers.
- Images (still or video) of pupils or their parents/carers should not be posted to social media sites.
- No comments should be made about the school, its staff or governors which are likely to cause offence or bring the school, its staff and governors into disrepute.
- Do not engage in online discussion on personal matters relating to members of the school community.
- 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

It is recognised that staff may, from time to time, socialise out of school and that images (still or video) or comments may be posted to social media sites at, or following, social events. Staff should exercise caution when making such posts to social networks and make careful consideration to whether such posts:

- will be seen by parents/carers ('open' or 'friends of friends' privacy settings)
- could be seen by others as bringing the profession into disrepute
- would upset/concern/anger colleagues who may appear in the posts

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 should 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 Online Safety Group to ensure compliance with the school policies.

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

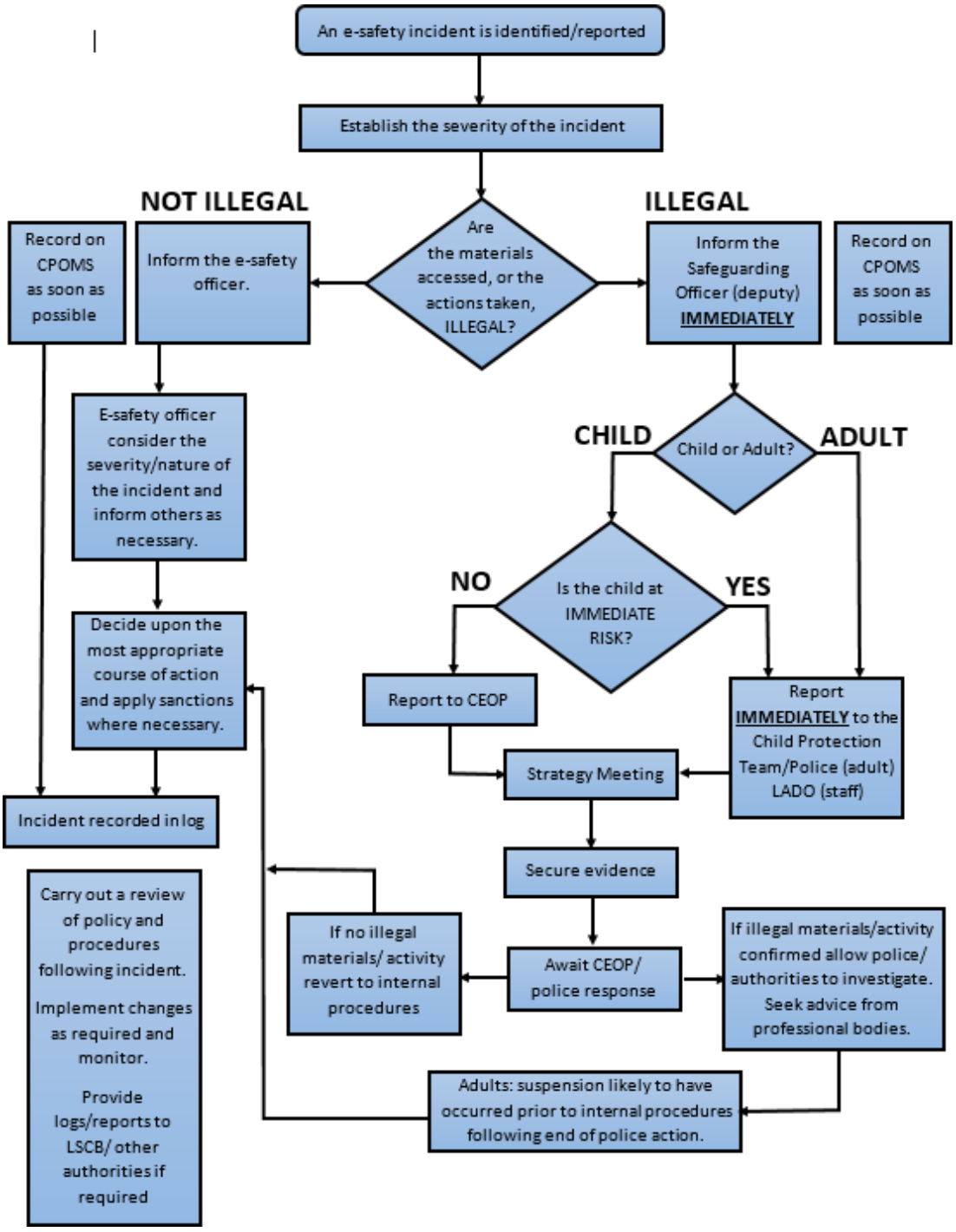
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism					X
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

	Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce (personal use on own devices at lunchtimes)			X		
File sharing (personal use on own devices at lunchtimes)			X		
Use of social media (personal use on own devices at lunchtimes)		X			
Use of messaging apps (personal use on own devices at lunchtimes)		X			
Use of video broadcasting e.g. Youtube		X			

Responding to Incidents

This procedure is intended for use when staff become aware of an e-safety incident. It is a clear, safe and secure approach to the management of incidents. Incidents might involve illegal or inappropriate activities (see "User Actions" above). If there is ANY suspicion that the incident may involve illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report **IMMEDIATELY**, and **in person** to the DSL/DDSL, recording the incident on CPOMS AS SOON AS POSSIBLE afterwards. For other incidents, report to the e-safety officer and record the incident on CPOMS.



Investigating Suspected Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- More than one senior member of staff will be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- The procedure will be conducted using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. The same computer will be used for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national/local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- The computer in question will be isolated. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures which may include the following actions:

Students / Pupils Incidents	Refer to class teacher	Refer to Senior Teacher/Deputy Head	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg Time Out / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X	X	X		X	X	X	X	X
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device		X	X			X	X	X	X
Unauthorised / inappropriate use of social media / messaging apps / personal email		X	X						
Unauthorised downloading or uploading of files		X	X			X	X	X	X
Allowing others to access school network by sharing username and passwords	X	X	X			X	X	X	X
Attempting to access or accessing the school network, using another pupil's account	X	X	X			X	X	X	X
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X			X	X	X	X

Students / Pupils Incidents (cont)	Refer to class teacher	Refer to Senior Teacher/Deputy Head	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg Time Out / exclusion
Corrupting or destroying the data of other users	X	X	X			X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X		X	X	X	X
Continued infringements of the above, following previous warnings or sanctions			X	X		X	X	X	X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school			X	X		X	X	X	X
Using proxy sites or other means to subvert the school's filtering system			X	X		X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident			X	X		X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material			X	X		X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X	X		X	X	X	X

Staff Incidents	Refer to line manager	Refer to Headteacher	Referral to Local Authority/LADO	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning – Verbal or Written	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X		X		X	X	X
Inappropriate personal use of the internet / social media / personal email		X	X			X	X	X
Unauthorised downloading or uploading of files	X	X				X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X			X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner		X				X	X	
Deliberate actions to breach data protection or network security rules		X			X	X	X	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X	X	X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X	X	X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		X	X	X	X	X	X	X
Actions which could compromise the staff member's professional standing		X			X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X			X	X	X	X

Staff Incidents (cont)	Refer to line manager	Refer to Headteacher	Referral to Local Authority/LADO	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning – Verbal or Written	Suspension	Disciplinary action
Using proxy sites or other means to subvert the school's / academy's filtering system		X			X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X				X		
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X	X	X
Accidentally accessing CSE material or abusive images of children and failing to report the incident		X				X		
Deliberately accessing or trying to access CSE material or abusive images of children		X	X	X	X	X	X	X
Accidentally accessing material that encourages discrimination on the grounds of a person's or group's gender, gender orientation, sexual orientation, race, religion or political affiliation and failing to report the incident		X				X		
Deliberately accessing or trying to access material that encourages discrimination on the grounds of a person's or group's gender, gender orientation, sexual orientation, race, religion or political affiliation		X	X	X	X	X	X	X
Accidentally accessing extremist/terrorist material and failing to report the incident		X				X		
Deliberately accessing or trying to access extremist/terrorist material		X	X	X	X	X	X	X
Breaching copyright or licensing regulations		X			X	X	X	X
Continued infringements of the above, following previous warnings or sanctions		X	X				X	X

Acknowledgments

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy Template and of the 360 degree safe Online Safety Self Review Tool:

- Members of the SWGfL Online Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Appendices

Pupil Acceptable Use Agreement

School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is 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.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Pupil Acceptable User Agreements will be completed:

- When a child enters the school in Reception – this will be the EYFS/KS1 Agreement and will be included as part of the Induction Pack distributed to all parents.
- When a child enters Year 3– this will be the KS2 Agreement and will be sent home with an accompanying letter.
- When a child is admitted to the school – this will be the AUP appropriate to the age of the child and will be included as part of the Induction Pack sent to all parents.

Staff Acceptable User Agreements will be completed as part of the induction of new staff to the school. New staff to the school will be given an IT Induction consisting of:

- The AUP
- Cybersecurity training
- Digital Safeguarding Training
- Overview of the school's systems – Laptop use, iPad, Microsoft 365, Google Classroom, Purple Mash, e-mail system

Parental Acceptable Use Policies will be completed by parents when their child enter the school, as part of the Induction Pack

Community Use Acceptable Use Policies will be completed as necessary, prior to any use of the school's systems

All Acceptable Use Policies will be re-issued to all relevant groups in the case of a change to their terms.

Pupil Acceptable Use Agreement (KS2)

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- I will never arrange to meet people off-line that I have communicated with on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for any other activity than that which my teacher(or other member of staff) has directed me.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will not bring my own personal devices (mobile phones/USB devices etc) into school unless there is an agreement between the school and my parents for me to do so. I understand that,

if I do bring my own devices into the school it will be stored on my behalf in the *sc*hool office during the school day until the end of the day when it will be returned to me.

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not use social media sites:
- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, time iut, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own equipment out of the school in a way that is related to me being a member of this school eg when communicating with other members of the school, accessing school email, Learning Platform, website etc.
-

Name of Pupil: .....

Class: .....

Signed: .....

Date: .....

Parent / Carer Countersignature: .....

Pupil Acceptable Use Agreement Policy (EYFS/KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

Signed (child): .....

Signed (parent): .....

This AUP is based on one produced by St Mark's Church of England / Methodist Ecumenical VA Primary School, Weston super Mare.

Parent Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name:.....

Pupil(s) Name(s):.....

As the parent/carer of the above pupils, I give permission for my child(ren) to have access to the internet and to ICT systems at school.

I know that my son/daughter has read (or had read to them) and signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school. .

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

The Head Teacher and office staff will have access to this form. Class Teachers will receive confirmation that your child has signed their Acceptable Use Agreement
This form will be stored in a secure place in the school office
This form will be stored for as long as your child is registered to attend Wilkinson Primary School
This form will be destroyed by shredding after your child has ceased to be registered to attend Wilkinson Primary School

Signed: .....

Date: .....

Use of digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publically shared by any means, only your child's first name will be used.

The school will comply with the Data Protection Act and request parents/carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act/GDPR) if permission is given at the start of the event by a senior leader (who will have checked permissions). To respect everyone's privacy, and in some cases for child protection, parents will be informed that these images should not be published or made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital / video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree.

Digital / Video Images Permission Form

Parent/Carers Name:..... Student / Pupil Name:.....

As the parent / carer of the above pupil

I agree to the school taking digital/video images of my child for use within the school.	Yes / No
I agree to the school taking digital/video images of my child for use on the school's website or any future social media platform	Yes/No
I agree to images of my child being taken by third parties (e.g. a journalist) for use in the local press	Yes / No
I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes / No

Signed: ..... Date: .....

This form (electronic or printed)	The images
The Head Teacher and office staff will have access to this form. Class Teachers will receive confirmation that your child has signed their Acceptable Use Agreement	The images may be published on the school website, in the local press or used around school.
This form will be stored in a secure place in the school office	School staff will have access to the original images.
This form will be stored for as long as your child is registered to attend Wilkinson Primary School	The original images will be stored on the hard drive of the school's server to which only staff have access and access can only be gained within school
This form will be destroyed by shredding after your child has ceased to be registered to attend the School	The original images will be stored for a maximum of the duration of your child's registered attendance at Wilkinson Primary School plus 7 years (to allow for images that may contain younger children to be preserved).
How the images will be destroyed	The original images will be destroyed by deleting the images from the camera's memory card or from the i-pad camera roll. The images will be removed from the hard drive of the school server by the technician who will ensure they cannot be recovered.
How you can request an image to be deleted	Any request for deletion of the images can be made, in writing, to the Headteacher (this includes removing the images from the school website).

Staff (Volunteer) Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is 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.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems and reports of potential issues will be notified to the Digital Safeguarding Lead and the Designated Safeguarding Lead and any issue may be further investigated.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, Microsoft 365, Google Classroom etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will use a strong password that is different to passwords used outside of school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.

- I understand that if I need to write down a password it should be stored where it is not possible that someone may steal it, and that I MUST NOT store my password or bitlocker code on the device or in the same bag that the device is carried in.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the Digital Safeguarding Lead and the Designated Safeguarding Lead.
- I understand that the safety and security of the devices I have been given are my responsibility. I will ensure that any device is transported locked, out of sight in the boot of a car or that I take extra care to ensure the device is with me at all times on public transport.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website, Twitter) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use electronic means to communicate with pupils. (Any electronic communication with parents / carers will use official school systems. Any such communication will be professional in tone and manner).
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will not upload comments/post/images to a social networking site that brings the school, its employees, pupils or governors into disrepute. I understand that whatever appears on my social networking platforms is solely my responsibility, no matter how it was caused.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops/tablets/mobile phones) in school, I will follow the rules set out in this agreement and in school policy, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I understand that the use of external mass storage devices (USB Memory Sticks/Pens, External Hard Drives) is prohibited in school.
- I will not use personal email addresses on the school ICT systems or as usernames for any online resource (E.g. Purple Mash etc).
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes) and I will report any suspicious e-mail activity immediately to the Digital Safeguarding Lead and the Designated Safeguarding Lead
- I will ensure that my data is regularly backed up, in accordance with relevant school policies (i.e. by ensuring that I properly shut down my laptop each evening).

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not try to use any programmes or software or other devices (Mobile phones, dongles etc) that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, , nor will I try to alter computer settings. If I wish for a particular programme to be installed I will discuss this with the school's technician and Computing Coordinator first.
- I will not disable or cause any damage to school equipment, or equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include verbal or written warnings, suspension, referral to the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school), my own devices and my use of communication technologies (text, e-mail, social networking sites (in school and when carrying out work related to the school) within these guidelines.

Staff / Volunteer Name: .....

Signed: .....

Date: .....

Community Users Acceptable Use Policy Agreement

This Acceptable Use Agreement is intended to ensure:

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

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices

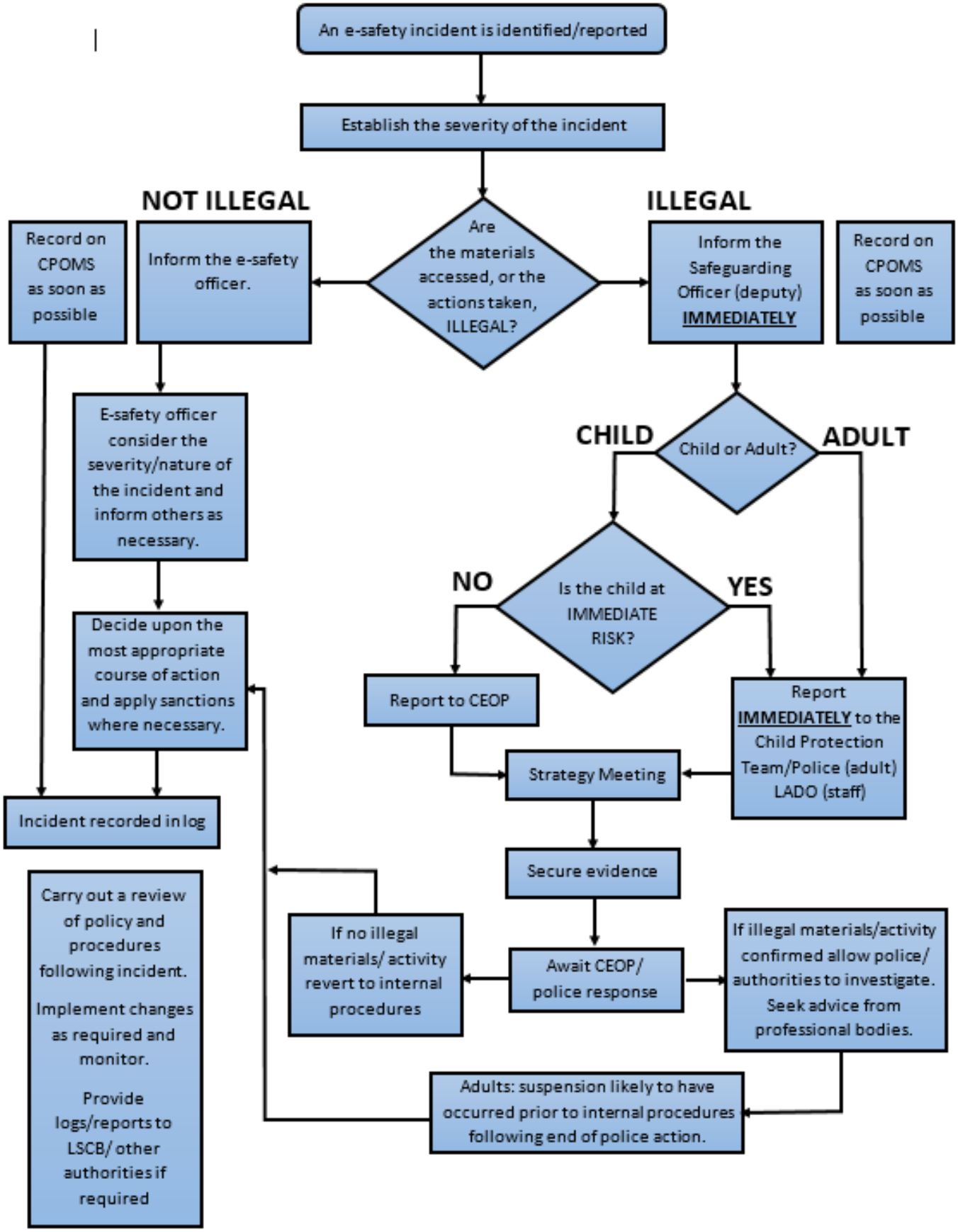
I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

The Headteacher, administration staff and the Online Safety coordinator will have access to this form.
This form will be stored in a secure locked place within the School's Office
This form will be stored for the duration of the use of the school's equipment
This form will be destroyed by shredding at the end of the use of the school's equipment

Name: ..... Signed: .....

Date: .....

Responding to incidents – Flow Chart



Record of reviewing devices/internet sites (responding to incidents of misuse)

Group: .....

Date: .....

Reason for investigation: .....

.....

.....

Details of first reviewing person

Name: .....

Position: .....

Signature: .....

Details of second reviewing person

Name: .....

Position: .....

Signature: .....

Name and location of computer used for review (for web sites)

.....

.....

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Training Needs Audit Log

Group: .....

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date

Use of Personal Device Log

Date	Person Requesting	Circumstances	What is to be stored (How Much)?	Date to be deleted by	Deletion confirmed?

School Policy: Electronic Devices – Searching & Deletion

Introduction

The changing face of information technologies and ever increasing pupil use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

The particular changes we deal with here are the added power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.

Items banned under the school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).

An item banned by the school rules may only be searched for under these new powers if it has been identified in the school rules as an item that can be searched for. There is a school policy which sets out clearly and unambiguously the items which:

- are banned under the school rules; and
- are banned AND can be searched for by authorised school staff

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The Head Teacher must publicise the school behaviour policy, in writing, to staff, parents/carers and pupils at least once a year.

http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

Relevant legislation:

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959

- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990

This is not a full list of Acts involved in the formation of this advice. Further information about relevant legislation can be found via the DfE.

Responsibilities

The Headteacher is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will normally be taken to Governors for approval. The Headteacher will need to authorise those staff who are allowed to carry out searches (Members of staff cannot be required to carry out such searches. They can each choose whether or not they wish to be an authorised member of staff).

This policy has been written by, and will be reviewed by, the Online Safety Coordinator

The Headteacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices: The Online Safety Coordinator, The Deputy Head Teacher, Senior Teachers. They can/will be assisted in a technical capacity by the School's Technician.

The Headteacher may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

Training / Awareness

Members of staff should be made aware of the school's policy on "Electronic devices – searching and deletion":

- at induction
- at regular updating sessions on the school's online safety policy

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data/files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Policy Statements

Search:
The school Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

Pupils are not allowed to bring mobile phones or other personal electronic devices to school or use them in the school.

If pupils breach these roles:

The device will be removed (securely stored) and only returned to the parents/carers.

The child will spend a period of time in 'Time Out'

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent - Authorised staff may search with the pupil's consent for any item
- Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for

In carrying out the search:

The authorised member of staff must have reasonable grounds for suspecting that a pupil is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for. (Whether there are 'reasonable grounds' is a matter decided on by reference to the circumstances witnessed by, or reported to, someone who is authorised and who exercises properly informed professional judgment and has received appropriate training).

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone/ personal electronic device before carrying out a search. (The powers included in the Education Act do not extend to devices owned (or mislaid) by other parties e.g. a visiting parent or contractor, only to devices in the possession of pupils).

The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the pupil being searched.

The authorised member of staff carrying out the search must be the same gender as the pupil being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the pupil being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a pupil of the opposite gender including without a witness present, **but only where they reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.**

Extent of the search:

The person conducting the search must not require the pupil to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

'Possessions' means any goods over which the pupil has or appears to have control – this includes desks, lockers and bags.

A pupil's possessions can only be searched in the presence of the pupil and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge. It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Members of staff may require support in judging whether the material is inappropriate or illegal. One or more Senior Leaders should receive additional training to assist with these decisions. Care should be taken not to delete material that might be required in a potential criminal investigation.

The school should also consider their duty of care responsibility in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such material can be most upsetting. There should be arrangements in place to support such staff. The school may wish to add further detail about these arrangements.

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so. (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. (It is recommended that members of staff should contact the Head Teacher for further guidance before taking action).

A record should be kept of the reasons for the deletion of data / files.

Care of Confiscated Devices

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage/loss of such devices (particularly given the possible high value of some of these devices).

The school may wish to add a disclaimer to the relevant section of the Behaviour Policy which may assist in covering the school against damage / loss claims.

Audit / Monitoring / Reporting / Review

The responsible person (Online Safety Coordinator) will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files. These records will be reviewed by the Online Safety Coordinator at least termly.

This policy will be reviewed by the head teacher and governors annually and in response to changes in guidance and evidence gained from the records.

Mobile Technologies Policy (inc. BYOD/BYOT)

Mobile technology devices may be a school owned/provided or privately owned smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

The absolute key to considering the use of mobile technologies is that the pupils, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school owned/provided or personally owned. The mobile technologies policy should sit alongside a range of polices including but not limited to the Safeguarding Policy, Bullying Policy, Acceptable Use Policy, policies

around theft or malicious damage and the Behaviour Policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen student learning, but they can also develop digital literacy, fluency and citizenship in students that will prepare them for the high tech world in which they will live, learn and work.

Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to your school network, filtering of personal devices, breakages and insurance, access to devices for all students, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership

Schools may consider implementing the use of mobile technologies as a means of reducing expenditure on school provided devices. However, it is important to remember that the increased network management costs and overheads involved in implementing this properly are likely to counterbalance or outweigh any savings.

The use of mobile technologies brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset. Before the school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

- The school Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies
- The school allows:

	School Devices		Personal Devices		
	School owned and allocated to a single user	School owned for use by multiple users	Pupil/ owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes		No	No
Internet only				No	No
No network access			Yes	Yes	

- The school has provided technical solutions for the safe use of mobile technology for school devices/personal devices.
    - All school devices are controlled though the use of Mobile Device Management software

- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access)
- The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user.
- All school devices are subject to routine monitoring
- Pro-active monitoring has been implemented to monitor activity

- When personal devices are permitted:
  - All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access
  - Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user, as does the liability for any loss or damage resulting from the use of the device in school
  - The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)
  - The school accepts no responsibility for any malfunction of a device due to changes made to the device if connection to the school network has been attempted or whilst resolving any connectivity issues
  - The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security
  - The school is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues

- Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition;
  - Visitors will be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements
  - Users are responsible for charging their own devices and for protecting and looking after their devices while in school
  - Personal devices should be charged before being brought to school as the charging of personal devices is not permitted during the school day
  - Personal devices must be in silent mode on the school site
  - School devices are provided to support learning.
  - Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
  - The changing of settings (exceptions include personal settings such as font size, brightness, etc…) that would stop the device working as it was originally set up and intended to work is not permitted

- The software / apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps
- The school will ensure that school devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to students on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.
- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately
- Photographing pupils on personal devices is not allowed under any circumstances.
- Devices may be used in lessons in accordance with teacher direction
- Staff owned devices should not be used for personal purposes during teaching sessions, unless there are exceptional circumstances
- Printing from personal devices will not be possible

Social Media Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils/students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by *the school*, its staff, parents, carers and children.

Scope

This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements.

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education
- Defines the monitoring of public social media activity pertaining to the school

The school respects privacy and understands that staff and pupils/students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

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

Digital communications with pupils are also considered.

Organisational Control

Roles & Responsibilities

- **SLT**
    - Facilitating training and guidance on Social Media use.
    - Developing and implementing the Social Media policy
    - Taking a lead role in investigating any reported incidents.
    - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
- **Staff**
    - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
    - Attending appropriate training
    - Ensure that posts/comments/images/videos uploaded to personal social media accounts do not bring the school, its employees, pupils or governors into disrepute.
    - Understand that whatever appears on their social networking platforms is their responsibility, no matter how it was caused.
    - Adding an appropriate disclaimer to personal accounts when naming the school

Monitoring

Whilst the active monitoring of personal social media accounts is not practical or even desirable the school has a duty to investigate any complaint made about the content of a social media post, using the procedures described in the Online Safety Policy/Acceptable Use Agreements

Behaviour

- **The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.**
- . Staff should not use social media to make ill-considered comments or judgments about the school, staff or pupils. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally, or with the involvement of the Local Authority or the LADO. Where conduct is considered illegal, the school will report the matter to the police and

other relevant external agencies, and may take action according to the disciplinary policy.

Handling abuse

- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- **Permission to use any photos or video recordings should be sought**. If anyone, for any reason, asks not to be filmed or photographed or for images/films of themselves not to be placed on a social media platform then their wishes must be respected.
- **Under no circumstances should staff share or upload student pictures online**
- If a member of staff inadvertently takes/posts a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- **Staff**
    - Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
    - 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.
- **Pupil/Students**
    - **Staff are not permitted to follow or engage with current or prior pupils of the school on any personal social media network account.**
    - The school's education programme should enable the pupils to be safe and responsible users of social media.
- **Parents/Carers**
    - **When parents/carers have access to a school online resource (Google Classroom/Purple Mash) where posting or commenting is enabled, parents/carers will be informed about acceptable use.**
    - Parents and carers are requested not to post ot social media platforms any images/videos they take of their children and others at school events such as sports days and performances
    - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- 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 should effectively respond to social media comments made by others according to a defined policy or process.

Appendix

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Acknowledgements

With thanks to Rob Simmonds of Well Chuffed Comms (wellchuffedcomms.com) and Chelmsford College for allowing the use of their policies in the creation of this policy.

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy:

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Internet Watch Foundation - https://www.iwf.org.uk/

CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE / Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
Netsmartz - http://www.netsmartz.org/

Tools for Schools

Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self review tool: www.360data.org.uk

Bullying / Online-bullying / Sexting / Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - http://enable.eun.org/
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – Cyberbullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harrassment
UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Digital Literacy & Citizenship curriculum

UKCCIS – Education for a connected world framework

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Mobile Devices / BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking

NEN - Guidance Note - BYOD

Data Protection

360data - free questionnaire and data protection self review tool

ICO Guide for Organisations (general information about Data Protection)

ICO Guides for Education (wide range of sector specific guides)

DfE advice on Cloud software services and the Data Protection Act

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Computing

ICO - Guidance we gave to schools - September 2012

IRMS - Records Management Toolkit for Schools

NHS - Caldicott Principles (information that must be released)

ICO Guidance on taking photos in schools

Dotkumo - Best practice guide to using photos

Professional Standards / Staff Training

DfE – Keeping Children Safe in Education

DfE - Safer Working Practice for Adults who Work with Children and Young People

Childnet – School Pack for Online Safety Awareness

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support

UKSIC – Appropriate Filtering and Monitoring

Somerset - Questions for Technical Support

NEN – Advice and Guidance Notes

Working with parents and carers

SWGfL Digital Literacy & Citizenship curriculum

Online Safety BOOST Presentations - parent's presentation
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops / education
The Digital Universe of Your Children - animated videos for parents (Insafe)
Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
Insafe - A guide for parents - education and the new media

Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011
Futurelab - "Digital participation - its not chalk and talk any more!"
Ofcom –Media Literacy Research

Glossary of Terms

AUP / AUA	Acceptable Use Policy / Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
WAP	Wireless Application Protocol
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.