Online Safety Policy (including E-Safety)

Adopted by Governing Body: 08.05.18

Reviewed by Governing Body: 11.05.21

Cycle of review: 1 year

Statutory Policy: No

Online Safety Co-ordinator: Mrs Trish Baker

Online Safety Governor: Steve Turner

Contents

Background and rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even more true for children/young people, who are generally much more open to developing technologies than many adults. In many areas, technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake, no more so than over the last year due to coronavirus (COVID-19) and the necessity for implementation of remote learning. Keeping pupils, students, and teachers safe during remote education is essential (Refer to Appendix 11 of the Safeguarding Policy).

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful, or inappropriate images or other content
- Allowing or seeking unauthorised access to personal information
- Allowing or seeking unauthorised access to private data, including financial data
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers.
- Online bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy, and relevance of information on the internet.
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive or addictive use which may impact on social and emotional development and learning.

This policy sets out how we strive to keep children safe whilst using technology. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures put in place to keep them safe) and so this policy also sets out how we educate children about the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends, and the wider community) to be aware and to assist in this process.

Our school's online safety policy has been written from a template provided by the South West Grid for Learning (SWGfL).

Development/ Monitoring/ Review of this policy

This online safety policy was developed by a working group made up of:

- School Online Safety Coordinator/ Deputy Head teacher
- Teachers
- Support Staff
- ICT Manager
- Online Safety governor

Consultation with the whole school community, for review of this policy, has taken place through the following:

- Dissemination to Staff and governors
- Shared with a sample of pupils from KS2 - 5

- Promoted to parents/carers to seek their views

Schedule for development/monitoring/review of this policy

The implementation of this online safety policy will be monitored by the	The Online Safety Co-ordinator /Headteacher/ SLT/ Governing Body
Monitoring will take place at regular intervals	At least annually
The governing body will receive regular reports on the implementation of the online safety policy (which will include anonymous details of online safety incidents) as part of a standing agenda item with reference to safeguarding	Half termly via meetings between the Designated Safeguarding Lead/Online Safety Co-ordinator and lead governor for online safety.
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technology, new threats to online safety or incidents that have taken place.	Annually
Should serious online safety incidents take place, the following external persons / agencies should be informed	Worcestershire Safeguarding Children Partnership online safety representative. Local Authority Designated Officer Worcestershire Education Adviser for Safeguarding Children in Education West Mercia 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 teaching staff, wider workforce, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital technology systems, **both in and out of school.**

The Education and Inspections Act 2006 empowers head teachers, 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 out of school, but are linked to membership of the school.

The 2011 Education Act increased these powers regarding 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 Section 4 of the Behaviour Policy.

The school will deal with such incidents using guidance within this policy as well as associated behaviour, safeguarding 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 & Responsibilities

This section begins with an outline of the online safety roles and responsibilities of individuals and groups within the school.

Governors

Governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the lead governor for online safety and the online safety co-ordinator who will review information about online safety incidents and report to the full governing board. A member of the governing body has taken on the role of online safety governor which involves:

- Termly conversations with the Online Safety Co-ordinator with an agenda on
    - Monitoring of online safety incident logs.
    - Reporting to relevant Governors committee's and meetings.

Head Teacher and Deputy Head Teacher

- The head teacher has a duty of care for ensuring the safety (including online safety) of all members of the school community, though the day-to-day responsibility for online safety is delegated to the Online Safety Co-ordinator
- The deputy head teacher (Designated Safeguarding Lead) receives and reviews the weekly output from monitoring software, and initiates action where necessary and provides regular reports to the Senior Leadership Team.
- The head teacher and deputy head teacher should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff, including non-teaching staff. (see flow chart on dealing with online safety incidents on page 22 and other relevant Local Authority HR / disciplinary procedures)
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

Online Safety Co-ordinator

Our Online Safety Coordinator is the person responsible to the head teacher and governors for the day-to-day issues relating to online safety. The online safety coordinator:

- 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.
- receives reports of online safety incidents as they occur and creates a log of incidents to inform future online safety developments.
- provides training and advice for staff.
- liaises with the Local Authority.
- liaises with school's ICT Network Manager.
- meets regularly with the lead governor for online safety to discuss current issues and review incident logs.
- attends relevant meetings and committees of the governing body.
- reports regularly to the Senior Leadership Team.
- receives appropriate training and support to fulfil their role effectively.

ICT Network Manager

The ICT manager is responsible for ensuring that:

- The school's digital infrastructure is as secure as possible and not open to misuse or malicious attack.

- The school meets the online safety technical requirements outlined on pages 10 - 19 of this policy (and any relevant Local Authority Online Safety Policy and guidance that may apply)
- Users only access Pitcheroak digital services, including hardware and software services through a secure means, on authorised devices and where relevant, with additional security measures such as Multi-Factor Authentication.
- Users keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant.
- The use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Online Safety Co-ordinator for investigation/action/sanction.
- Monitoring software/systems are implemented and updated as agreed in school policies.

Classroom Based Staff
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 safeguard the welfare of children and refer child protection concerns using the proper channels: **this duty is on the individual, not the organisation or the school.**
- They have read, understood, and signed the school's Acceptable Use Agreement for staff (see Appendix 1C)
- They report any suspected misuse or problem to the Headteacher/ Online Safety Co-ordinator/ ICT Network Manager for investigation/ action/ sanction.
- All digital communications with pupils/ parents/ carers is on a professional level and only carried out using official school systems
- 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.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They actively monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies regarding these devices.
- In lessons where internet use is pre-planned pupils are 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.

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

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, where appropriate
- 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 other digital devices. 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

School Council

The school council will discuss issues relating to online safety and when appropriate the staff representatives ask the school online safety coordinator to attend meetings. Issues that arise are referred to other school bodies as appropriate and when necessary, to bodies outside the school such as the Worcestershire Safeguarding Children Partnership.

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' evenings, newsletters, letters, website, social media, and information about national/local online safety campaigns/literature. 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/Learning Platform
- their children's personal devices in the school (where this is allowed)

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/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the continuous help and support of the school to recognise and avoid online safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

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

- A planned online safety programme is provided as part of ICT/computing, PHSE and other lessons as appropriate to the needs of pupils. This is regularly revisited, covering the use of ICT and new technologies both in school and outside school.
- Key online safety messages will be reinforced through further input via assemblies and pastoral activities, taking part in national initiatives form example National Online Safety day as well as informal conversations when the opportunity arises.
- Where appropriate, pupils should 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.

- Where appropriate, pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Pupils should 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 include ensuring that children are safe from terrorist and extremist material on the internet*.
- 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 can freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit, encouraging them to discuss anything of which they are unsure and implementing the expected sanctions and/or support as necessary. Staff should take appropriate measures by using remote screen monitoring software to monitor the pupil's device usage throughout the lesson.
- Pupils will be made aware of what to do should they experience anything, while on the Internet, which makes them feel uncomfortable.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g., racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

The contribution of pupils to the school's online learning strategy

It is our general school policy to encourage pupils to play an active role in shaping the way our school operates and this is very much the case with our online learning strategy. Pupils often use technology out of school in ways that we do not in school and members of staff are always keen to hear of children's experiences and how they feel the technology (especially rapidly developing technology such as mobile devices) could be helpful in their learning.

Education – Parents/carers

Parents and carers understanding of online safety risks and issues will be variable, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents/carers 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:

- Parent engagement activities
- Letters, newsletters, web site, Learning Platform.
- Parents/carers evenings/sessions
- High profile events/campaigns e.g., Safer Internet Day

- Reference to the relevant web sites/publications such as Childnet, SWGFL and Safer Internet Org (Refer to Appendix 4).

Education - The Wider Community
Community Users are not permitted to access the school's digital system. However, the school will provide opportunities for 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 (through the National Online Safety portal)
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community.

Education and training - Staff/ Volunteers
It is essential that all staff – including non-teaching 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. An audit of the online safety training needs of all staff will be carried out regularly. (The National Online Safety portal includes access to a range of modules.)
- 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 which are signed as part of their induction.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The ICT Network Manager is CEOP trained.
- The Online Safety Co-ordinator, ICT Network Manager and ICT subject leader will receive regular updates through attendance at external training events (e.g. from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Online Safety Coordinator, ICT Network Manager or ICT subject leader will provide advice, guidance and training as required to individuals as required on an ongoing basis.

External support for training, including input to parents/carers, is sought from appropriately qualified persons when required.

Training - Governors
Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee or group involved in technology, online safety, health and safety or safeguarding. This may be offered in several ways:

- Attendance at training provided by the Local Authority (Governor Services or School Improvement Service), National Governors Association or other relevant organisations.
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

Whole School approach and links to other policies
This policy has strong links to other school policies as follows.

Online Safety Policy	How we strive to ensure that all individuals in school stay safe while using Learning Technologies. The online safety policy constitutes a part of the ICT policy.
GDPR and Data Protection Policy	How we categorise, store and transfer sensitive and personal data and protect school systems. This links strongly and overlaps with the online safety policy.
Anti-bullying	How school strives to eliminate bullying – link to online bullying
PSHE	Online Safety has links to staying safe
Safeguarding	Safeguarding children electronically is an important aspect of Online Safety. *The online safety policy forms a part of the school's safeguarding policy*
Behaviour	Positive strategies for encouraging online safety and sanctions for disregarding it.

Technical – infrastructure/equipment, filtering and monitoring

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 need 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 (these may be outlined in Local Authority or other relevant body policy and guidance)
- 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 (at KS2 and above) will be provided with a username and secure password by the ICT Network Manager who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password. (Class logons and passwords are used for KS1 and below)
- The "master/administrator" passwords for the school systems, used by the ICT Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g., school safe)
- The ICT Network Manager 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 (child sexual abuse images) is filtered by the broadband or filtering 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. N.B. additional duties for schools under the Counter Terrorism and Securities Act 2015 include ensuring that children are safe from terrorist and extremist material on the internet. (see appendix 3 for information on "appropriate filtering").
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc)
- The ICT Network Manager will monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. All access logs,

including sign ins and access to file storage is logged within the security and compliance module of Microsoft Azure AD. In addition, the school will use other systems (such as Smoothwall monitor) to monitor keyboard input on devices.

- Users can report any actual/potential technical incident/security breach to the ICT Network Manager via the IT helpdesk.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, client devices, mobile devices, etc, including strong password policies, Multifactor Authentication, and firewall restrictions. These will help to protect the school accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up-to-date virus software.

Password Security and Authentication

The school's online safety curriculum will include frequent discussion of issues relating to password security and staying safe in and out of school. Where appropriate, the ICT Network Manager will provide secure passwords based on current government guidance on complexity for pupils, in order to maintain network security.

Staff will also be required to use Multifactor Authentication to access school services to enhance network security and help prevent malicious attack.

Internet Filtering and Firewall

The school purchases connectivity services from a private limited company, and layer a Smoothwall firewall and filtering appliance to ensure all inbound and outbound connections are monitored. In addition, compatible devices are also linked to Smoothwall Cloud Filter, which provides internet filtering even if the device is taken off site.

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so.

Internet Filtering and Firewall Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by ICT Network Manager (with ultimate responsibility resting with the head teacher and governors). They manage the school filtering in line with this policy and keep logs of changes to and breaches of the filtering system.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the standard there must be a way to log and report these changes.

All users have a responsibility to report immediately to class teachers / online safety coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered. Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education / training / awareness

Pupils are made aware of the importance of filtering systems through the school's online safety education programme (see Education – pupils' section of this policy on page 7).

Staff users will be made aware of the filtering systems through:

- signing the Acceptable Use Agreement (as part of their induction process)
- briefing in staff meetings, training days, memos etc. (timely and ongoing).
- Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions / newsletter etc.

Changes to the filtering system

Where a member of staff requires access to a website that is blocked for use at school, the process to unblock is as follows:

- The teacher makes the request to the ICT Network Manager via the IT helpdesk.
- The ICT Network Manager checks the website content to ensure it is appropriate for use in school.
- The ICT Network Manager completes a Charge Request Form (CRF) and reference the helpdesk ticket number, which is filed for future reference.

The ICT Network Manager will need to apply a rigorous policy for approving / rejecting filtering requests. This can be found in Appendix 3 but the core of this should be based on the site's content:

- The site promotes equal and just representations of racial, gender, and religious issues.
- The site does not contain inappropriate content such as pornography, abuse, racial hatred, and terrorism.
- The site does not link to other sites which may be harmful / unsuitable for pupils.
- If the ICT Network Manager is unsure of any websites, advice must be sought from the DSL's.

Monitoring

The school will therefore monitor the activities of users on the school network and on school equipment.

Monitoring takes place as follows:

- The online safety co-ordinator reviews the monitoring console captures weekly, with email/call alerts from Smoothwall if someone is in immediate danger.
- Potential issues are referred to an appropriate person depending on the nature of the capture.
- Teachers are encouraged to identify in advance any word or phrase likely to be picked up regularly through innocent use (e.g., 'goddess' is captured frequently when a class is researching or creating presentations on the Egyptians) so that the word can be allowed for the period of the topic being taught.

Audit / reporting

Filter change-control logs and incident logs are made available to:

- the governor with responsibility for online safety within the timeframe stated in the governor responsibilities section on page 5 of this policy.
- the Worcestershire Safeguarding Children Partnership on request

This filtering policy will be reviewed, with respect to the suitability of the current provision, in response to evidence provided by the audit logs.

Personal data security (and transfer)
This is dealt with in detail in the school's GDPR and Data Protection Policy.

Mobile Technologies including BYOD(Bring Your Own Device)/ BYOT (Bring Your Own Technology)
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 utilizing 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, behavior policy, bullying policy, acceptable use 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 programmed.

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. Pupils 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 pupils that will prepare them for the high-tech world in which they will live, learn and work.

Considerations

There are several 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 pupils, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership.

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 and parents/carers will consider the use of mobile technologies, however the school does not routinely allow staff to access digital services provided by Pitcheroak School on personal devices.

Any devices which are connected to the school's network must be verified by the ICT Network Manager. The ICT Network Manager may find reasonable reason to reject adding the device to the schools networking, including (but not limited to)

- Lack of security on client device
- Inability to install certificates (for HTTPS inspection)

If a personal device has been permitted, it can be retracted at any time by the ICT Network Manager.

Regarding personal mobile phones, members of staff are free to use these devices outside teaching time and away from pupils however are not permitted to use these devices for engaging in off-site activities where students are present. A school mobile phone will be provided in these cases.

Pupils are not currently permitted to bring their personal handheld devices into school. These must be handed in at the beginning of the day and not collected until the end of the day.

Liability

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 (and their parents/carers) 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 while on the school network or whilst resolving any connectivity issues.

In addition:

- Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition.
- Devices may not be used in tests or exams
- Visitors should 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 keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network, for example by using client network isolation.
- Users are responsible for charging their own devices and for protecting and looking after their devices while in the school
- Personal devices should be charged before being brought to the school as the charging of personal devices is not permitted during the school day
- Devices must be in silent mode on the school site
- School devices are provided to support learning. It is expected that pupils will bring devices to the school as required.
- 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 always easily accessible. 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 devices contain the necessary apps for schoolwork. Apps added by the school will remain the property of the school and will not be accessible to pupils 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.
- Devices may be used in lessons in accordance with teacher direction.
- Printing from personal devices will not be possible.

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 online bullying 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). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers can take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken using school equipment; **the personal equipment of staff should not be used for such purposes.**
- 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.
- Staff should be aware of pupils for whom it has been deemed inappropriate to take and share / publish their photograph (e.g., some looked after children)
- 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.
- Pupils' full names will not 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 parents or carers.

Data Protection

Please refer to the schools GDPR and Data Protection policy.

School data is only permitted to be stored on school owned devices, and authorised services provided by digital services, such as OneDrive and SharePoint.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- Never store any school related data on USB sticks, external hard drives or other non-removable media.
- will not transfer any school personal data to personal devices except as in line with school policy
- access personal data sources and records 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

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:

Communication Technologies	Staff & other adults				Pupils			
	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	x	x				x		
Use of mobile phones in lessons				x				x
Use of mobile phones in social time		x						x
Taking photos on personal mobile phones/cameras				x				x
Use of other mobile devices e.g., tablets, gaming devices		x				x		
Use of personal email addresses in school for school purposes				x				x
Use of personal emails in school for personal purposes		x						x
Use of messaging apps for school purposes (e.g., WhatsApp)			x					x

Use of social media			x				x	
Use of blogs		x					x	

Access to email is provided for all users in school via Office 365 which is managed by the ICT Network Manager.

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 and pupils 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 their class teacher / online safety coordinator/ICT Manager – in accordance with the school policy (see page 19 – 21), the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and they must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- All students from EYs to KS5 will be provided with an online account, however only students in KS2 and above will have email activated.
- Pupils normally use only their email account to communicate with people outside school and with the permission / guidance of their class teacher
- A structured education program is delivered to pupils which helps them to be aware of the 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.

Social Media – Protecting Professional Identity

Protecting Professional Identity (Refer to Working in Worcestershire Schools including Code of Conduct the school's Social Media guidelines and 'Teachers Standards 2012 for teachers' professional conduct)

Schools and the local authority have a duty of care to provide a safe learning environment for pupils and staff and 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, race or disability or who defame a third party may render the school or local authority 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 should ensure that:

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

When official school social media accounts are established there should 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 disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media account. 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

Monitoring of Public Social Media:

The school's use of social media for professional purposes will be checked regularly by the Headteacher and ICT Manager to ensure compliance with the school policies.

- 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

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 from school and all other technical systems. 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
Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 Refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					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	
Activities that might be classed as cyber-crime under the Computer Misuse Act: Gaining unauthorised access to school networks, data and files, through the use of computers/devices Creating or propagating computer viruses or other harmful files Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) Disable/Impair/Disrupt network functionality through the use of computers/devices Using penetration testing equipment (without relevant permission) Schools will decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent young people becoming involved in cyber-					x

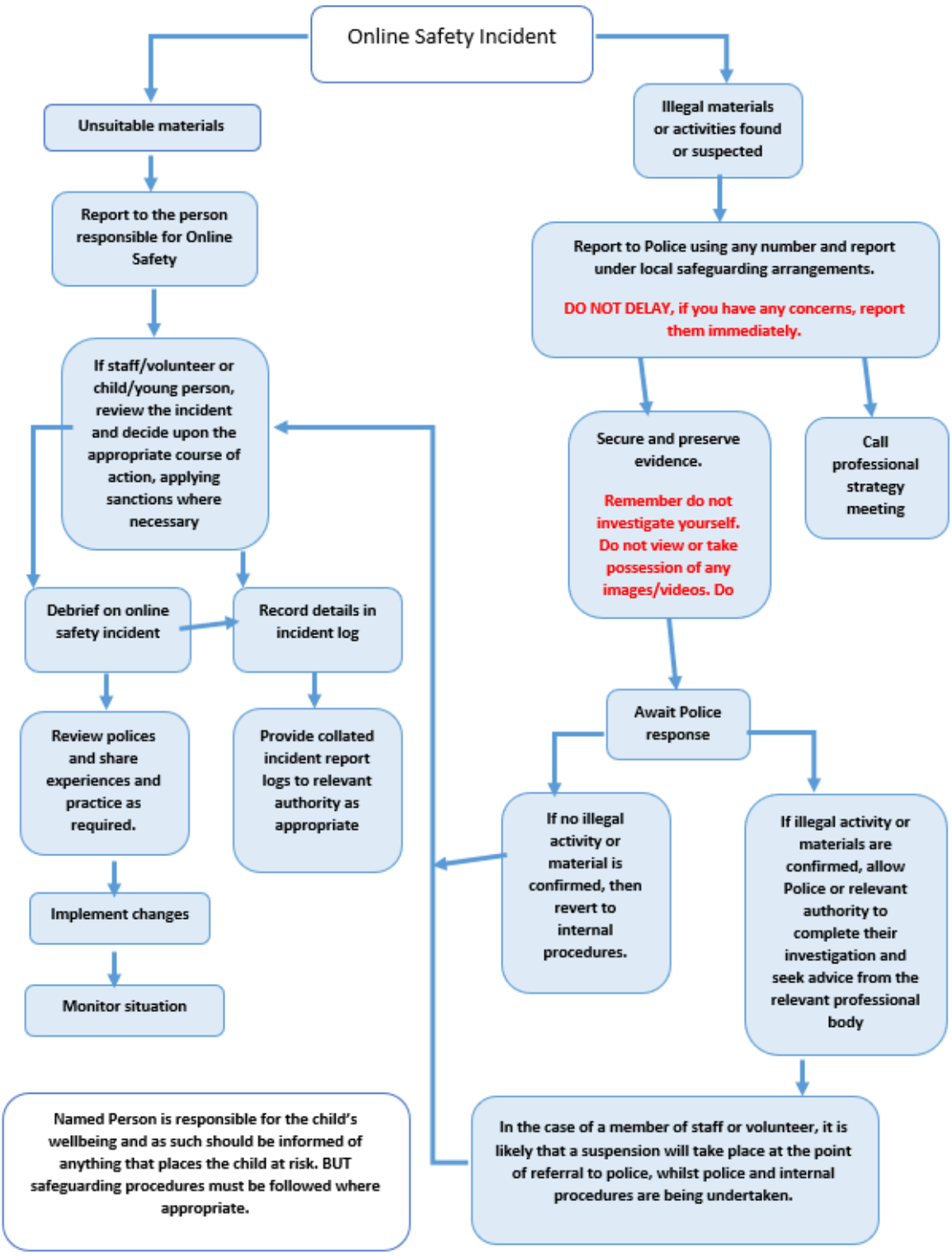
crime and harness their activity in positive ways – further information here					
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				x	
Revealing or publicising confidential or proprietary information (e.g., financial/personal information, databases, computer/network access codes and passwords)				x	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				x	
Using school systems to run a private business				x	
Infringing copyright				x	
On-line gaming (educational)	x				
On-line gaming (non-educational)				x	
On-line gambling				x	
On-line shopping/commerce		x			
File sharing			x		
Use of social media			x		
Use of messaging apps				x	
Use of video broadcasting e.g., Youtube				x	

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Other 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:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure 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. Use the same computer 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
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. 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 as follows:

Pupil Incidents	**Actions/Sanctions**								
	Refer to class teacher	Refer to the online safety co-ordinator	Refer to Headteacher	Refer to Police	Refer to ICT manager for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction e.g., detention/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	x	x	x	x	x	x
Unauthorised use of non-educational sites during lessons	x				x				
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	x					x	x		
Unauthorised/inappropriate use of social media/ messaging apps/personal email	x	x			x	x		x	
Unauthorised downloading or uploading of files	x				x		x	x	
Allowing others to access school network by sharing username and passwords	x	x	x		x		x	x	
Attempting to access or accessing the school network, using another student's/pupil's account	x				x		x		
Attempting to access or accessing the school network, using the account of a member of staff	x	x	x		x			x	
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	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		x	
Using proxy sites or other means to subvert the school's filtering system	x	x	x		x	x	x	x	

Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x		x	x			
Deliberately accessing or trying to access offensive or pornographic material	x	x	x		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		

Staff Incidents	**Actions/Sanctions**							
	Refer to line manager	Refer to Headteacher	Refer to Local Authority/HR	Refer to Police	Refer to ICT Manager	Warning	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	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	x	
Careless use of personal data e.g., holding or transferring data in an insecure manner	x	x	x		x	x		x
Deliberate actions to breach data protection or network security rules	x	x	x		x	x	x	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		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	
Using personal email/ social networking/ instant messaging/ text messaging to carrying out digital communications with students/ pupils	x	x			x			
Actions which could compromise the staff member's professional standing	x	x						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x	x				x		
Using proxy sites or other means to subvert the school's filtering system	x	x			x	x		x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x			x	x		

Deliberately accessing or trying to access offensive or pornographic material	x	x	x		x	x	x	x
Breaching copyright or licensing regulations	x					x		
Continued infringements of the above, following previous warnings or sanctions	x	x			x			x

Appendices

Appendix 1 – Acceptable Use Agreements

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to school systems.

Acceptable Use Agreements are provided in Appendix 1 of this policy for:

- Pupils
- Staff (Volunteers are not permitted to access the school ICT system)
- Technical support personnel

Acceptable Use Agreements are signed by all pupils from Key Stage 1 upwards, where appropriate. Pupils resign on entering a new Key Stage.

All employees of the school sign when they take up their role in school and in the future if significant changes are made to the policy.

Parents sign once when their child enters the school. The parents' policy also includes permission for use of their child's image (still or moving) by the school, permission for their child to use the school's ICT resources (including the internet) and permission to publish their work.

Community users sign when they first request access to the school's wireless network.

Induction policies for all new members of staff include this guidance.

Note: The acceptable use agreements below may be adapted to work correctly with digital means of collection (e.g., Microsoft Forms) if the content of the agreement stays the same.

Appendix 1A Acceptable Use Agreement for KS2 (and KS1 where appropriate)

This is how we stay safe when we use computers:

- I will ask an adult if I want to use the computer/ipad
- I will only use activities if an adult says it is OK.
- I will take care of the computer and other equipment
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will turn off the monitor and tell an 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/ipad.

I understand these computer rules and will do my best to keep them.

My Name	
Signed (Child)	

Appendix 1B Acceptable Use Agreement for KS3, KS4 and KS5

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 access to these digital technologies.

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 students/pupils to agree to be responsible users.

I understand that while I am a member of Pitcheroak School I must use technology in a responsible way.

For my own personal safety:

- I understand that my use of technology (especially when I use the internet) will be supervised and monitored.
- I will keep my password safe and will not use anyone else's (even with their permission)
- I will keep my own personal information safe as well as that of others.
- I will be aware of "stranger danger" when I am communicating on-line.
- I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.
- For the safety of others:
- I will not interfere with the way that others use their technology.
- I will be polite and responsible when I communicate with others,
- I will not take or share images of anyone without their permission.

For the safety of the school:

- I will not try to access anything illegal, inappropriate or that will cause harm or distress to others.
- I will not download anything that I do not have the right to use.
- I will only use my own personal device if I have permission and use it within the agreed rules.
- I will not deliberately bypass any systems designed to keep the school safe.
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes of any type on the devices belonging to the school without permission.
- I will only use social networking, gaming and chat through the sites the school allows.

I understand that I am responsible for my actions and the consequences and that the school will act if I am involved in inappropriate behaviour. I understand that if I don't follow this rule, action taken may include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

My name:	Signed (pupil):	Date:

Appendix 1C Acceptable Use Agreement for Staff and Volunteers
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 always have an entitlement to safe access to the internet and digital technologies.

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 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. I recognise the value of the use of digital technology for enhancing learning and will ensure that 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 digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g., laptops, email, learning platform) 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 in the online safety policy.
- 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 I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate, or harmful material or incident of which I become aware, to the appropriate person.

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.
- Where images are published (e.g., on the school website / learning platform) I will ensure that it will not be possible to identify by name, or other personal information, those who are featured. (see Use of digital and video images on page 15)
- I will only use social networking sites in school in accordance with the school's policies. (see Social Media section on page 18)
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (see sections A.3.1 and A.3.2 of the online safety policy)
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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.

- I will only use my personal mobile ICT devices as agreed in the online safety policy (see Mobile Technologies page 13) and then with the same care as if I was using school equipment. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems
- I will not use any form of removable media (USB stick, external hard drives) and will only use appropriate means of transferring data (OneDrive, Sharepoint)
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist 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 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, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where digital personal data is transferred outside the secure school network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I will not take or access pupil data, or other sensitive school data, off-site without specific approval. If approved to do so, I will take every precaution to ensure the security of the data.
- 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 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 school.

- I understand that this Acceptable Use Agreement 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 out of school and to my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could involve a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police (see Dealing with unsuitable/inappropriate activities page 19).

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) within these guidelines.

Staff/ Volunteer Name	
Signed (Child)	
Date	

Appendix 1D Acceptable Use Agreement for Parent/Carer

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 always have an entitlement to safe internet access. This Acceptable Use Agreement 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 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 about 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.

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

Child's name:	
Parent/Carer signature:	
Parent/Carer signature:	
Date:	

Permission for my child to use the internet and electronic communication.

As the parent/ carer of the above pupil(s), I give permission for my son/ daughter to have access to the internet and to ICT systems at school.

I know that my son/ daughter has signed an Acceptable Use Agreement (where appropriate) 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 ICT 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 ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of this agreement.

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.

Parent/Carer signature:	
Date:	

Appendix 2 – Guidance for Reviewing Internet Sites

This guidance is intended for use when the school needs to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might typically include online bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking sites, messaging sites, gaming sites or blogs etc.

Do not follow this procedure if you suspect that the website(s) concerned may contain child abuse images. If this is the case, please refer to the Flowchart for responding to online safety incidents and report immediately to the police. Please follow all steps in this procedure:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure 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. Use the same computer 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. *This will automatically be done by Smoothwall Monitor.* It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These can be uploaded to CPOMS
- 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
    - Isolate the computer in question as best you can. Any change to its state may affect a later police investigation.
    - It is important that all of the above steps are taken as they will provide an evidence trail for the group, possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Appendix 3 – Criteria for website Filtering

ORIGIN - What is the website's origin?

- The organisation providing the site is clearly indicated.
- There is information about the site's authors ("about us", "our objectives", etc.)
- There are contact details for further information and questions concerning the site's information and content.
- The site contains appropriate endorsements by external bodies and/or links to/from well-trusted sources

CONTENT - Is the website's content meaningful in terms of its educational value?

- The content is age-appropriate
- The content is broadly balanced in nature, and does not appear unduly biased, partisan or unreliable
- The site is free of spelling mistakes, grammatical errors, syntax errors, or typos.
- The site promotes equal and just representations of racial, gender, and religious issues.
- The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.
- The site does not link to other sites which may be harmful / unsuitable for the pupils
- The content of the website is current.

DESIGN - Is the website well designed? Is it / does it:

- appealing to its intended audience (colours, graphics, layout)?
- easy to navigate through the site - links are clearly marked etc?
- have working links?
- have inappropriate adverts?

ACCESSIBILITY - Is the website accessible?

- Does it load quickly?
- Does the site require registration or passwords to access it?
- Is the site free from subscription charges or usage fees?

Appendix 4 – Links to other organisations and documents

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

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

Revenge Porn Helpline - https://revengepornhelpline.org.uk/

Internet Watch Foundation - https://www.iwf.org.uk/

Report Harmful Content - https://reportharmfulcontent.com/

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 Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

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

SWGfL Test filtering - http://testfiltering.com/

UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/

SELMA – Hacking Hate - https://selma.swgfl.co.uk

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 Evolve - https://projectevolve.co.uk

UKCCIS – Education for a connected world framework

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Data Protection

360data - free questionnaire and data protection self review tool

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

DfE advice on Cloud software services and the Data Protection Act

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

SWGfL Safety & Security Resources

Somerset - Questions for Technical Support

NCA – Guide to the Computer Misuse Act

NEN – Advice and Guidance Notes

Working with parents and carers

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

Internet Matters

Prevent

Prevent Duty Guidance

Prevent for schools – teaching resources

NCA – Cyber Prevent

Childnet – Trust Me

Research

Ofcom –Media Literacy Research

Further links can be found at the end of the UKCIS Education for a Connected World Framework

Appendix 5 – Glossary of Terms

AUP/AUA Acceptable Use Policy/Agreement – see templates earlier in this document

CEOP Child Exploitation and Online Protection Centre (part of National Crime Agency, 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

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.

UKSIC UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

UKCIS UK Council for Internet Safety

VLE Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

WAP Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS Education for a Connected World Framework