FALCONHURST SCHOOL

E-SAFETY POLICY

Annual Review to Governors: October 2024

Scheduled Review Date: October 2025

Contents

RATIONALE

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. Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties.

This policy applies to all aspects of ICT (especially the following areas) and is informed by the DfE Online Safety Guidance (June 2019), Keeping Children Safe in Education (KCSIE annual update) and the principles and practice of the following school policies: Social Networking, Code of Conduct, Data Protection (GDPR), Safeguarding, Health and Safety, Behaviour (including anti-bullying) PSHE. Collectively, these documents provide guidance on:

- Websites
- All electronic communication including e-mail, Instant Messaging and chat rooms
- All Social Media, including Facebook and Twitter
- Mobile phones, Smartwatches, tablets and other mobile devices with web functionality
- Gaming, especially online
- Blogging and Vlogging
- Sending nude and semi-nude images
- Podcasting, Video Broadcasting & Music Downloading
- Responding to breaches of this policy

Whilst exciting and beneficial both in and out of the context of education, ICT is continually being developed, so cannot necessarily be easily and constantly policed. All users need to be aware of the range of risks associated with the use of these technologies. We understand the responsibility to educate our pupils on e-safety issues in order to enable them to remain both safe and legal within and beyond the classroom.

The Education and Inspections Act 2006 empowers Headteachers to such an 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 (see appendix for template policy). 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:

Governors

As e-safety is an important aspect of strategic leadership within the school, the Governors and Headteacher have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Board has taken on the responsibility of Online Safety under their remit of Safeguarding. This role will include:

- regular meetings with the Online Safety Lead
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors

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 Lead.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority/MAT/other relevant body 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.
- 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.
- Leaders will actively remind parents to be vigilant around/avoid PEGI 12+ games, social media platforms and apps in order to collectively safeguard children.
- That all new staff receive information on the Staff Code of Conduct 2020 and Social Networking Policy 2021 for Falconhurst Staff as part of their induction and will sign that they have read, understand and accept the policy.

Designated Safeguarding Leads

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

The DSLs take responsibility for any concerns that arise from filtering and monitoring events passed on by the E-Safety lead.

E-Safety Lead

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- Verifies the monitoring and filtering logs frequently and passes on any concerns to the relevant members of staff, primarily the DSLs.
- Ensures that the monitoring tool is tailored and up-to-date with current trends and concerns locally, nationally and internationally.
- 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
- Co-Ordinates E-Safety Pupil Legends who assist in securing, analysing and evaluating E-Safety systems and the impact of teaching on pupil learning and behaviours.
- Liaises with school technical staff and receives reports of online safety incidents to create a log of incidents which informs future online safety developments.
- Meets annually with the online safety governor to discuss current issues, review incident logs and filtering/change control logs
- Reports to senior leadership team upon request
- Communicates with families to understand their views and needs
- Actively reminds families to be vigilant around/avoid Pegi 12+ games, social media and apps in order to collectively safeguard children.

IT Manager (contractor)

Those with technical responsibilities are responsible for ensuring that:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack
- The school meets required online safety technical requirements and any local authority or government safety policy/guidance that may apply.
- Users may only access the networks and devices through a properly enforced password protection policy
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- 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
- The use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the headteacher, senior leaders and online safety lead for investigation/action/sanction
- Monitoring software/systems are implemented and updated as agreed in school policies

- ICT equipment issued to staff is logged and serial numbers are recorded as part of the school's inventory. A record of equipment issued and signed for is kept by the School Business Manager

All staff

Security:

- All usernames and passwords to Management Information Systems and other school software must be kept secure. This information must not be shared and should be changed regularly.
- All school staff users must keep all school related data secure (in accordance with Data Protection, Code of Conduct and Acceptable Use policies). This includes all personal, sensitive, confidential or classified data or information contained in documents copied, scanned or printed.
- Staff must avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles.
- On termination of employment, resignation or transfer, staff must return all ICT equipment to the school and a signed record kept. Staff must also provide details of all their system logons so that they can be disabled.

Safeguarding (personal and pupil):

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices
- They are vigilant and report any concerns immediately regarding pupils' safety and take every opportunity to remind pupils that agreeing to meet people or giving personal information through e- mail or the internet can be a risk

Conduct:

- All staff must comply with the Social Networking Policy 2024 regarding the posting of any information or images relating to the school.
- Read, have understood and signed the staff Acceptable Use Policy 2024
- Report any suspected misuse, abuse or problem to the Headteacher/Senior Leader/Online Safety Lead/IT Manager for investigation/action/sanction
- Ensure that all digital communications with pupils/parents/carers are professional and only carried out using official school systems
- Whilst in school, the school does not allow any access to social networking sites other than the school's own Facebook or Class Dojo page where general information is available for the whole school community and the Twitter feed for live school sports fixtures and updates.

Email:

- Use the email account provided by school for **all** school business. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed. Note: The

use of e-mail within school is an essential means of communication. In the context of school, e-mail should not be considered private
- Whenever school e-mail is accessed, (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.
- For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account office@falconhurstschool.co.uk should be the account that is used for all school business and as an initial contact for any whole school or wider community business
- Actively manage their school email accounts as these are subject to disclosure in response to a request for information under the Freedom of Information Act 2000. This covers such acts as: deleting all emails of short-term value, effective folder organisation, frequent housekeeping of folders and archives
- Unknown, Malicious or Suspicious emails are not to be opened or forwarded. These are to be reported to ithelpdesk@falconhurstschool.co.uk for security checks.

Teaching and Support Staff Specifically

Are responsible for ensuring that:

- Online safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the e-safety charter, E-Safety Policy and the Pupil Acceptable Use Policies
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They are actively reminding children and parents to be vigilant around/avoid PEGI ratings for games, apps and social media platforms.
- They monitor the use of digital technologies, mobile devices, Smartwatches, 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. Filtered safe search engines should also be used, such as squiggle and raw searches should be actively discouraged
- if Internet research is set for homework, specific sites will be suggested that have previously been checked. Parents should be advised to supervise any further research

Pupils:

Security:

- Are responsible for keeping their passwords secure and appropriate for their age

Safeguarding:

- Need to understand the importance of immediately reporting abuse, misuse or access to inappropriate materials to trusted adults (Teacher, Parent, Childline CEOP button)
- Will be expected to know and understand expectations on the use of mobile devices, Smartwatches and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- Are aware of the impact of cyber bullying and know how to seek help if they are affected by any form of online bullying
- Understand PEGI ratings for games and apps as a tool for understanding their suitability.
- May only use school-approved email accounts on the school system and only under direct teacher supervision for educational purposes

Conduct:

- All pupils are responsible for using the school digital technology systems in accordance with the student/pupil acceptable use agreement
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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
- Are expected to adhere to the generally accepted rules of 'netiquette' particularly in relation to the use of appropriate language and not reveal any personal details about themselves or others in e-mail communications

Pupils with Additional Needs

The school endeavours to create a consistent dialogue with parents for all pupils and this in turn should aid establishment and future development of the school's e- safety rules. However, staff will be aware of some pupils and families who may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.

Where a pupil has been identified with social understanding needs, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities will be carefully planned and managed to ensure all children receive resources that are meaningful and age appropriate.

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices/Smartwatches 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 and on-line student/pupil records
- their children's personal devices in the school (where this is allowed)
- supervising online homework or home learning this work and further research.

EDUCATION AND TRAINING PURPOSE STATEMENTS

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 help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety is a focus across all areas of the curriculum and staff are expected to regularly reinforce online safety messages within relevant lessons. Our online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

- A mapped, sequenced and planned online safety curriculum (ILearn2 and support materials)
- E-Safety focus days with whole school, phase and class-based assembly themes

Alongside this, pupils are taught to:

- Be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Be aware of, and build 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.
- Understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- To access sites checked as suitable for their use and reassured that processes are in place for dealing with any unsuitable material that is found in internet searches.
- To freely search the internet whilst staff maintain vigilance in monitoring the content of the websites visited
- 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 IT 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.

Staff/Volunteers

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

- A planned and audited programme of formal online safety training will be made available to staff, this may utilise The National College or other recognised and reputable providers.
- All new staff receive this policy and associated safeguarding documents as part of their induction programme
- The Online Safety Lead (or other nominated person) 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.
- The Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

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, Class Dojo links
- Parents/carers evenings/sessions
- 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

Training – Governors

Governors, specifically the Governor responsible for E-Safety, should participate in online safety training/awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/ National Governors Association/or other relevant organisation (e.g. SWGfL).
- Participation in school training/information sessions for staff or parents

SAFE AND PROFESSIONAL CONDUCT, OFF AND ON-LINE

a) Mobile Technologies (Including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, Smartwatch, 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. All use of mobile technologies is subject to

relevant school polices including but not limited to the safeguarding policy, behaviour 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 programme.

- The school acceptable use agreements for staff, pupils/students and parents/carers considers the use of mobile technologies
- The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*			
Internet only						
No network access				*Yes*	*Yes*	*Yes*

b) 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 in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

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 are allowed to take digital/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 on 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.
- 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.
- Photographs and film of pupils engaged in school activities can only be stored on school systems and not published on social media without explicit permission of parents/carers. Only first names will be used and no information leading to the identification of a pupil will be provided.
- Pupils are not permitted to use personal digital equipment, including mobile phones, Smartwatches and cameras in school.
- Staff must have permission from the Headteacher before any image can be uploaded for publication.

c) Sharing Platforms

With the increased use of the internet, and sharing platforms in particular, the Falconhurst Community is aware of the implications of sharing information on these platforms. Therefore,

- The use of the school logo on any personal web pages is not permitted.
- Using material from any copyrighted source without permission is likely to breach copyright and is therefore not permissible.
- The school reserves the right to require removal of any material published by any member of the Falconhurst Community, or wider which may adversely affect the school's reputation or create risk of legal proceedings against the school.
- We do not include or use any school, data, information, contact details or photographs of employees, pupils, parents or partner organisations without the explicit written permission of the school and the explicit written permission of the data subject (e.g. person shown in any photograph).
- We do not include comments or photographs which could bring into question the school's credibility.

- It is against the school's policy for staff members to accept as 'friends' on social networking sites any child or vulnerable adult
- If staff receive press or media contact regarding the content of their personal site and feel there may be implications for them or which in any way relates to the school, they must consult the Headteacher.

d) Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers that 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	ved with staff permission	Not allowed
Mobile phones may be brought to the school	X				X			
Use of mobile phones in lessons			X					X
Use of mobile phones in social time	X							X
Taking photos on mobile phones/cameras		X					X	
Use of other school mobile devices e.g. tablets, gaming devices		X					X	
Use of personal mobile devices e.g. Smartwatch, tablets	X							X
Use of personal email addresses in school, or on school network		X						X
Use of school email for personal emails				X			X	
Use of messaging apps		X					X	
Use of social media		X					X	
Use of blogs		X					X	

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 the nominated person – in accordance with the school policy, 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
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs 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.
- Pupils will be taught about online safety issues, such as the risks attached to the sharing of personal details. They will also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information will not be posted on the school website and only official email addresses will be used to identify members of staff.

e) 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, race or disability or who defame a third party may render the *school* or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides a clear policy for all staff on managing their online presence (Social Networking Policy) and this must be read in conjunction with this E-Safety Policy.

BREACHES and INCIDENT REPORTING

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Policy or Behaviour Policy which could also lead to criminal or civil proceedings.

The school's 'Whistleblowing Policy' and 'Child Protection and Safeguarding Policy' can support any member of staff or pupil to report any incident of concern.

E-Safety is the responsibility of all members of the Falconhurst community. Any concerns should be reported to the Designated Safeguarding Leader.

Defining Unsuitable/Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is obviously banned from school and all other technical systems. Other activities e.g. cyber-bullying is banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but are 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:

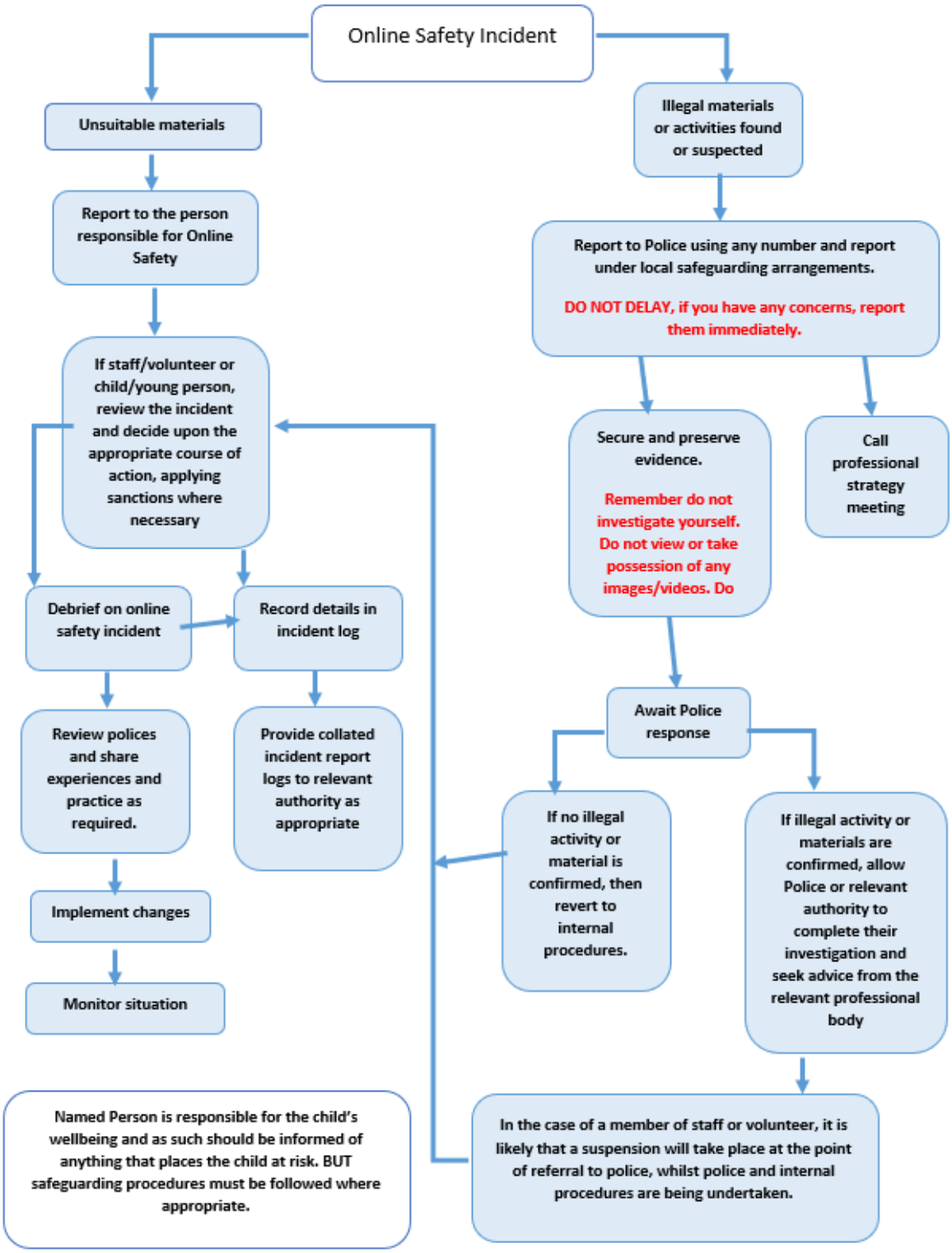
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual 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	
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)						X
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

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 and Sanctions

It is more likely that we 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:

	Actions/Sanctions								
Pupils Incidents	Refer to class teacher/tutor	Refer to Phase Leader	Refer to Headteacher	Refer to Police and/or MASH	Refer to technical support staff for action	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			
Unauthorised use of non-educational sites during lessons	X				X	X	X	X	X
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	X	X	X	X		X	X	X	X
Unauthorised/inappropriate use of social media/ messaging apps/personal email	X	X	X	X	X	X	X	X	X
Unauthorised downloading or uploading of files	X	X	X	X	X	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	X	X	X	X
Attempting to access or accessing the school network, using the account of a member of staff		X	X		X				
Corrupting or destroying the data of other users	X	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			
Continued infringements of the above, following previous warnings or sanctions		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			
Using proxy sites or other means to subvert the school's/academy's filtering system		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			
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X	X	X		X			

	Actions/Sanctions							
Staff Incidents (arising from activity logs or staff disclosure)	Refer to phase manager	Refer to Headteacher	Refer to HR/ LADO/ MASH	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Possible Warning[1]	Suspension[1]	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
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	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	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	X	X
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with pupils		X	X	X		X	X	X
Actions which could compromise the staff member's professional standing		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/academy'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
Breaching copyright or licensing regulations	X	X	X		X	X	X	X
Continued infringements of the above, following previous warnings or sanctions		X	X	X	X	X	X	X

[1] Referral to Disciplinary Policy

SAFEGUARDING AND DATA PROTECTION

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 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 (Staff and Pupils) will be provided with a username and secure password by the IT Manager/ Class Teacher who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master/administrator" passwords for the school systems, used by the IT Manager (or other person) must also be available to the Headteacher or School Business Manager (SBM) and kept in a secure place (held by Partnership Education).
- The IT 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
- Internet access is filtered for all users. Illegal and/or inappropriate content 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 aims to ensure that children are safe from terrorist and extremist material when accessing the internet
- The school has provided enhanced/differentiated user-level filtering
- School technical staff regularly monitor and record the activity of users on the school technical systems and 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 devices are protected by up to date virus software.
- An agreement is in place (Guest Wi-Fi System Use) for the provision of temporary access of "guests" (e.g. supply teachers, visitors) onto the school systems.

- An agreed policy is in place (Acceptable Use Policy) regarding the extent of personal use that users (staff/pupils/community users) and their family members are allowed on school devices that may be used out of school.
- An agreed system is in place (Acceptable Use Policy and IT Manager has to authorise) that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place (Acceptable Use Policy) regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. *Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.*

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. For details refer to the School's Data Protection Policy (GDPR).

When personal data is stored on any mobile device or removable media the:

- data must be encrypted and password protected.
- device must be password protected.
- device must be protected by up to date virus and malware checking software
- 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 must ensure that they:

- 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 where personal data is stored and that mobile or other devices (including USBs) these must be encrypted and password protected.
- 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

DEVELOPMENT/MONITORING/REVIEW OF THIS POLICY

This online safety policy has been developed by a working group at Falconhurst School made up of:

- Headteacher
- E-Safety Lead
- Governors

Schedule for Development/Monitoring/Review

This online safety policy is approved by the Governing Board	*Annually every Summer Term*

The implementation of this online safety policy will be monitored by the:	*ICT Leader* *Senior Leadership Team,*
Monitoring will take place:	*At least termly*
The Governing Board will receive a report on the implementation of the online safety policy:	*Annually in the Safeguarding report*
Should serious online safety incidents take place, the following external persons/agencies should/may be informed:	*Designated Safeguarding Lead, Safeguarding Governor, 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 from Webadmin
- Internal monitoring data for network activity
- Surveys/questionnaires of
    - pupils
    - parents/carers
    - staff

APPENDIX 1 ~ PUPIL ACCEPTABLE USE AGREEMENT – KS2

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 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 *pupils* to agree to be responsible users.

Acceptable Use 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.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- 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 use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.
- 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 only use my own personal devices (mobile phones/Smartwatch etc.) in school if I have permission. I understand that, if I do use my own devices in the *school*, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- 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 only use social media sites with permission and at the times that are explicitly agreed upon.

When using the internet for research or recreation, I recognise that:

- 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 online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could 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.

Please complete the following sections 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.

Student/Pupil Acceptable Use Agreement Form

This form relates to the pupil acceptable use agreement; to which it is attached.

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 devices in the *school* (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this *school* e.g. communicating with other members of the school, accessing school email, website etc.

Name of Student/Pupil: .....

Group/Class: .....

Signed: .....

Date: .....

Parent/Carer Countersignature .....

APPENDIX 2 ~ PUPIL ACCEPTABLE USE AGREEMENT – KS1 and EYFS

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 computers/tablets 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): .....

APPENDIX 3 ~ PARENT/CARER 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 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 agreement 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: .....

Student/Pupil Name(s): .....

As the parent/carer of the above pupils, 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 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 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.

Signed: .....

Date: .....

APPENDIX 4 ~ CONSENT FOR USE OF DIGITAL/VIDEO IMAGES & CLOUD SYSTEMS

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 publicly shared by any means, only your child's first name/initials will be used.

The school will comply with the Data Protection Act and request parent's/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 in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.

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:..... Pupil Name:.....

As the parent/carer of the above pupil, I agree to the school taking digital/video images of my child/children.	Yes/No
I agree to these images being used:	
• to support learning activities.	Yes/No
• in open publicity/Social Media that reasonably celebrates success and promotes the work of the school.	Yes/No
• On our secure Class Dojo Class and School App	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: .....

Use of Cloud Systems Permission Form

The school uses Google for pupils and staff. This permission form describes the tools and pupil/student responsibilities for using these services.

The following services are available to each pupil as part of the school's online presence:

- Gmail (Google's email service)
- Google Classroom

Using Google will enable your child to collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils and members of staff. These services are entirely online and available 24/7 from any internet-connected computer.

The school believes that use of the tools significantly adds to your child's educational experience.

Do you consent to your child to having access to this service?		Yes/No
Pupil Name:		
Parent/Carers Name:		
Signed:	Date:	

APPENDIX 5 ~ LEGISLATION and GUIDANCE

Schools should be aware of the legislative framework under which this E-Safety policy and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to erase or amend data or programs without authority; obtain unauthorised access to a computer; "eavesdrop" on a computer; make unauthorised use of computer time or facilities; maliciously corrupt or erase data or programs; deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The Data Protection Act 2018

Updates the 1998 Act and incorporates the General Data Protection Regulations (GDPR)

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. The school reserves the right to monitor its systems and communications in line with its rights under this act.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom.

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

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.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress.

Links to other organisations or documents for teacher advice and guidance

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/

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

CEOP - http://ceop.police.uk/

ThinkUKnow - https://www.thinkuknow.co.uk/

LGfL – Online Safety Resources

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

Netsmartz - http://www.netsmartz.org/

Bullying/Online-bullying

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

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

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

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

DfE advice on Cloud software services and the Data Protection Act

ICO Guidance on taking photos in schools

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

The National College - https://thenationalcollege.co.uk/courses/online-safety-for-schools

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

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 6 ~ 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
MAT	Multi Academy Trust
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