Online Safety Policy

Policy Review: January 2024

Date for next review: January 2026

Signed Head teacher:

Signed Chair of Governors:

Contents

Online Safety Policy

Scope of the Policy

This policy applies to all members of the Yealmpton School community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.

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

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix). 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 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

The following section outlines the online safety roles and responsibilities of individuals/ groups within the *school*:

Governor Board

Governors are responsible for the approval of the online 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 role of Online Safety Governor and this role is combined with that of the Child Protection/Safeguarding Governor)

The role of the Online Safety Governor will include:

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

Headteacher and Senior Leaders

- The Online Safety Group: Headteacher, Assistant Headteacher, Computing Lead & Safeguarding Governor
- 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 Senior Leaders 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. (Appendix flow chart online safety incidents)
- 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.
- 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.

Online Safety Lead

The Online Safety Lead role is combined with the Designated Safeguarding Lead role (supported by the Deputy Safeguarding Officers:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority and WeST Trust relevant body
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments, (Appendix :suitable log sheets).
- meets regularly with Online Safety *Governor* to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of Governors
- Monitors this policy regularly with the Senior Leadership Team
- Any online incidents will be dealt will be the responsibility of the Online Safety and School Behaviour Leaders

WeST Trust Network Manager/Technical staff

The school has a managed ICT service provided by WeST , it is the responsibility of the WeST Trust IT Team to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school technical staff. The WeST IT Team as the managed service provider are fully aware of the school online safety policy and procedures.

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
- that the *school* meets required online safety technical requirements and any *Local Authority /MAT/other relevant body* online safety policy/guidance that may apply.
- that 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 (see appendix "Technical Security Policy ")
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Senior Leaders; Online Safety Lead for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the school online safety policy and practices
- they have read, understood and signed the staff acceptable use policy/agreement (AUP/AUA)
- they report any suspected misuse or problem to the Headteacher, Senior Leader/Online Safety Lead for investigation/action/sanction
- all digital communications with students/pupils/parents/carers should be 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 monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead and Deputy 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

Online Safety Group

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

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

- the production/review/monitoring of the school online safety policy/documents.
- mapping and reviewing the online safety/digital literacy curricular provision –(relevance, breadth & progression)
- monitoring network/internet/filtering/incident logs
- consulting stakeholders – including parents/carers and the students/pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool when appropriate

Appendix : An Online Safety Group Terms of Reference

Pupils:

- to use 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
- to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *school's* online safety policy covers their actions out of school.

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 and on-line pupil records
- their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems or programmes as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

Appendix: A community users acceptable use agreement (AUA).

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

In planning their online safety curriculum schools to refer to DfE Teaching Online Safety in Schools

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 curriculum should be provided as part of Computing/PHSE/other lessons
- Key online safety messages should be reinforced as part of a programme of assemblies/ pastoral activities
- 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.
- 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 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.
- Duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely (guided) search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) 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.

Education – 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
- 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

Education – The Wider Community

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

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community

- Sharing their online safety expertise/good practice with other local schools
- Education & Training – Staff/Volunteers

Staff online safety training:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced..
- 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.
- Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding.

Technical – infrastructure/equipment, filtering and monitoring

The WeST IT Team 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:

Technical Security Policy

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements and works closely with the WeST IT Team. (See appendix :Technical Security Policy
- 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.
- Class logons and passwords for F/KS1/KS2 and below will be grouped but the school remains aware of the associated risks.
- The "master/administrator" passwords for the school systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated Senior Leader/School Administrator and kept in a secure place (e.g. school safe or locked cupboard
- School Administrator and Headteacher are 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.
- 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.
- The WeST Trust IT Team provide appropriate user-level filtering .
- The WeST Trust IT Team 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.
- The Administrators will provide temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- *Staff predominately use school devices for school use and occasional personal use outside of school.*
- *This policy forbids staff from downloading executable files and installing programmes on school devices.*

- *Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured*.

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

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, 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.

Mobile Technologies Policy

The school acceptable use agreements for staff, pupils/ and parents/carers will give consideration to the use of mobile technologies

	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*	*No Hand into office*	*Yes Only during staff breaks Only away from children*	*No Handed into school office*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*NO*
Internet only	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*No*
No network access	*No*	*No*	*No*	*No*	*No*	*No*

Aspects that the school may wish to consider and be included in their online safety policy, mobile technologies policy or acceptable use agreements:

School owned mobile devices:

- *Name teacher - School trips*
- *If personal use is allowed- No*
- *Levels of access to networks –No*
- *Levels of access to internet – appropriate school business*
- *WeST IT Team =Management of devices/installation of apps/changing of settings/monitoring*
- *WeST IT Team - Network/broadband capacity*
- *Technical support*
- *Filtering of devices*
- *Access to cloud services*
- *Data Protection*
- *Taking/storage/use of images*
- *Exit processes – what happens to devices/software/apps/stored data if user leaves the school*
- *Liability for damage*
- *Staff training*

Personal devices:

- Which users are allowed to use personal mobile devices in school (Staff or Educational visitors)
- Restrictions on where, when and how they may be used in school (Staff breaks and away from children)
- Storage –Locked cupboard during lessons
- Staff will be allowed to use personal devices for school business –Only to make emergency contact with school

[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.

- Levels of access to networks/internet (as above)Network/broadband capacity
- Technical support (no technical support is available)
- Filtering of the internet connection to these devices
- Data Protection- Follow guidelines
- The right to take, examine and search users devices in the case of misuse (England only) – N.B. this must also be included in the Behaviour Policy.
- Taking/storage/use of images – No images to be taken on site or school trip
- Liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility).
- Identification/labelling of personal devices
- Visitors will be informed about school requirements-Administrator on arrival at school)
- Jigsaw PSHE programmes of study - about the safe and responsible use of mobile devices is included in the school online safety education programmes.

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/academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *students/pupils* in the digital/video images.
- 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.

Communications

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

	Staff & other adults			Students/Pupils				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	wed with staff permission	Not allowed
Mobile phones may be brought to the school/academy Staff		✓						
Use of mobile phones in lessons				✓				
Use of mobile phones in social time Staff		✓						
Taking photos on mobile phones/cameras personal No				✓				
Use of other mobile devices e.g. tablets only		✓				✓		
Use of personal email addresses in school/academy, or on school/academy network		✓		✓				
Use of school/academy email for personal emails (Ocaasional)		✓			✓			
Use of messaging apps		✓		✓				
Use of social media		✓			✓			
Use of blogs		✓			✓			

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 MS Teams)*
- 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, 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.*

- *Pupils will have access to remote learning via the school system of MS Teams.*
- *Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
- *Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

The school has a duty of care to provide a safe learning environment for pupils and staff.

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

- Ensuring that personal information is not published
- Training 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 should be made in social media to pupils, parents/carers or school/academy staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school /academy
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school/academy 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/academy disciplinary procedures*

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, 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

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others when appropriate
- The *school's* use of social media for professional purposes will be checked regularly by the safeguarding team and Online Safety Group to ensure compliance with the school policies.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned 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:

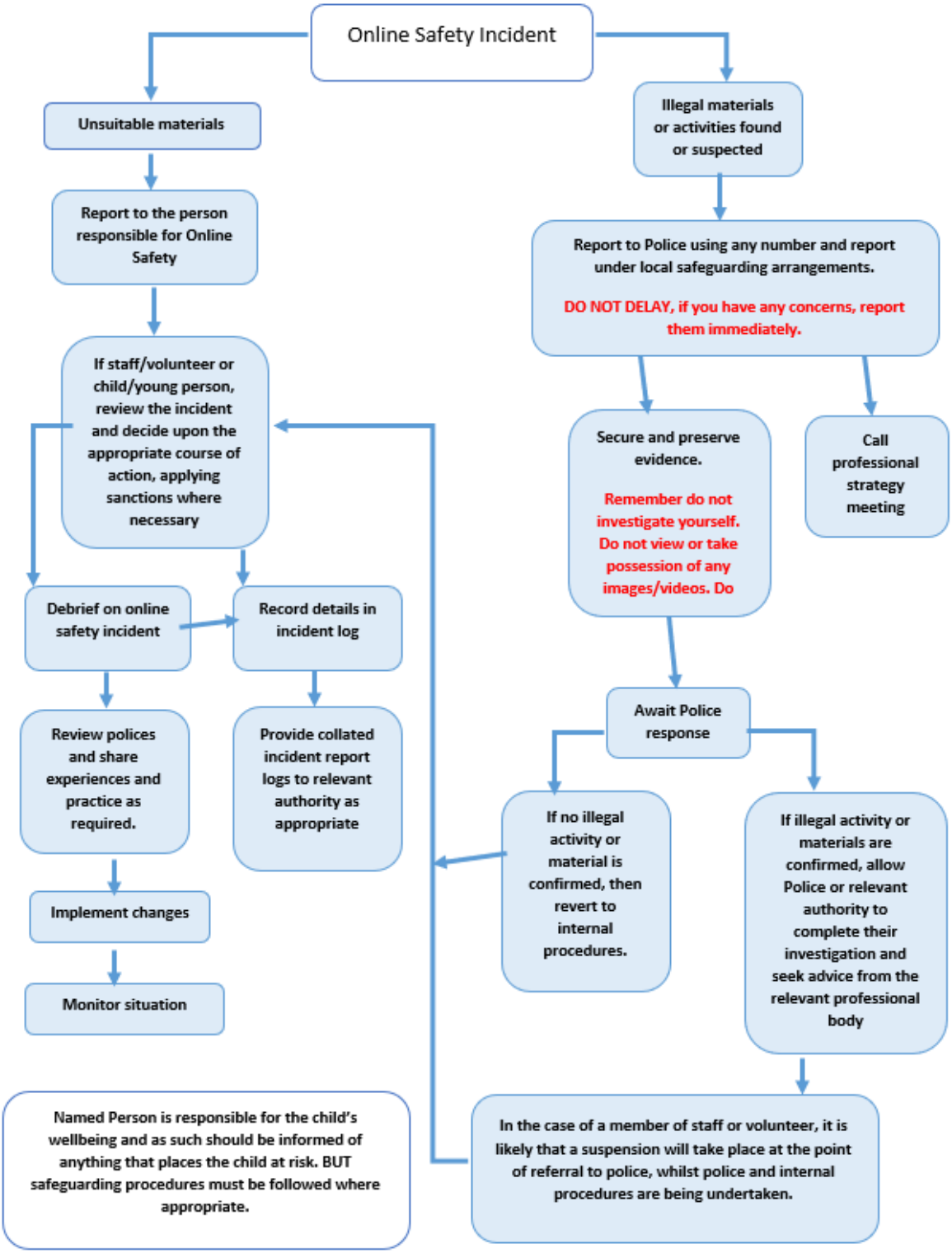
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child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



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/Academy Group 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:

	Actions/Sanctions								
Pupils Incidents	Refer to class teacher/tutor	Refer to \senior leader	Refer to Headteacher/Assistant Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction 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					
Unauthorised use of non-educational sites during lessons	X	X	X			X			
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	X	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		X			
Allowing others to access school/academy network by sharing username and passwords	X	X	X	X		X			
Attempting to access or accessing the school/academy network, using another student's/pupil's account	X	X	X	X		X			
Attempting to access or accessing the school/academy 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			
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X		X			
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X		X			
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school	X	X	X	X		X			
Using proxy sites or other means to subvert the school's/academy's filtering system	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			
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	Refer to line manager	Refer to Headteacher Principal	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	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				
Inappropriate personal use of the internet/social media/personal email		X	X					
Unauthorised downloading or uploading of files		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					
Careless use of personal data e.g. holding or transferring data in an insecure manner		X	X					
Deliberate actions to breach data protection or network security rules		X	X					
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X					
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X					
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils		X	X					
Actions which could compromise the staff member's professional standing		X	X					
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school/academy		X	X					
Using proxy sites or other means to subvert the school's/academy's filtering system		X	X					
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X					
Deliberately accessing or trying to access offensive or pornographic material		X	X					
Breaching copyright or licensing regulations		X	X					
Continued infringements of the above, following previous warnings or sanctions		X	X					

Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from:

SWGfL Online Safety Policy Templates

Appendices

Pupil Acceptable Use Agreement – Key Stage 2 Pupils

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 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 primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- 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 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 not use my own personal devices (mobile phones/USB devices etc.) in school.
- I understand that, if I do bring my own decide to school I need to hand it in to the office.
- 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 allowed .

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, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the acceptable use agreement. By returning this agreement access will be granted to school systems and devices.

Pupil Acceptable Use Agreement Form

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

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. Please sign with agreement of your parent/ carer and return this agreement, to enable access to be granted to school systems. Parents are asked to read and discuss the agreement and raise awareness through education programmes

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, 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, VLE, website etc.

Name of Pupil: .....

Parent /Carer Counter signature : .....

Group/Class: .....

Signed: .....

Date: .....

Pupil Acceptable Use Policy Agreement – for Foundation/KS1 Pupils

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 follow the rules when using Remote Learning MS Teams
- 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

Name of child: .....

Signed (parent): .....

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

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 and to access remote learning via MS Teams.

Key Stage 2

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.

Foundation and Key Stage 1

I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have 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.

As the school/academy is collecting personal data by issuing this form, it should inform parents/carers as to:

- School Staff (teachers, Senior Leaders and Admin) will have access to the electronic form
- Stored securely in office systems
- Stored until your child leaves primary school and deleted

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

Use of Digital/Video Images

There are sometimes occasions when we wish to take photographs or make video recordings of pupils at our school. Sometimes this is strictly for educational purposes and on other occasions it may be for other purposes related to the running of the school (e.g. taking photographs for use in brochures and the school's and Trust's social media pages and websites). Similarly, there are occasions when the local press visit the school to record particular events (e.g. Children in Need or the new Foundation classes starting school) and they may wish to publish photographs of children in newspapers or use recordings of the children on television when reporting these events.

In order to comply with General Data Protection Regulations, the school needs your specific consent before taking photographs or making video recordings of your child for purposes which are not part of its core activities. We would therefore be grateful if you could answer the questions overleaf, sign each section, date the form and return it to us by Wednesday 23rd September 2020.

Conditions of Consent

An Images Consent Database is kept in School showing parents' and carers' preferences with regard to the use of their child's image and name (as expressed on the Images Consent Form). Where a consent form is not held for a child, the school will not use their image.

The database will be consulted before images or names are used for any publicity purpose.

If consent has been given for all purposes, no further consent will be sought.

If consent has not been given, the parent or carer may be approached for permission to use their child's image either one time only, or in group photos, or in all future photos. The database will be updated accordingly.

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. The school will not risk the imaging of vulnerable children. Only images of children in appropriate dress will be used.

First names of pupils may be used in Press Releases and on the School's and Trust's websites as specified in the Images Consent Database.

Names will only be used in publicity where individual pupils are being congratulated on their achievements. Every attempt will be made to avoid identifying pictured pupils by name.

At any time, a parent or carer has the right to withdraw any or all consent previously given. This removal of consent will be actioned by the school without reasonable delay upon the submission of a signed letter requesting 'Withdrawal from Consent'.

Images w ill be deleted after use or in the case of the school's website or brochures kept with consent forms until they are no longer required.

These Conditions of Consent are available on the school's website for your reference.

MAGES CONSENT

(Please complete in BLOCK CAPITALS)

Pupil Surname: ..... Date Completed:.....

Pupil Forename: ..... Pupil's Date of Birth: .....

Parent/Carer Name: .....

In order to comply with General Data Protection Regulations, the school needs your consent before taking photographs or making video recordings of your child for purposes which are not part of its core activities.

We would be grateful if you could answer all of the following questions after reading the conditions of consent document overleaf. Each statement requires a signature to confirm preference.

		Parent/Carer Signature
I agree that the school can take photographs of my child which may be used in the school and Trust literature (e.g. newsletters, brochures, displays and other promotional material etc).	Yes / No	
I agree that the school and Trust can use images of my child on its website. (Please note the website can be viewed across the world).	Yes / No	
I agree that the school and Trust can use images of my child on its social media pages (such as Facebook and Twitter).	Yes / No	
I agree that the school can use images of my child in video recordings to promote the school and Trust, within the local community.	Yes / No	
I agree that the school can take photographs and make video recordings of my child for the school and Trust's own records and archives (e.g. photographs of sports team).	Yes / No	
I agree that my child can appear in video recordings or in collections of photographs, held on digital storage, which the school may make of school events and which it may sell to parents and carers of children at the school to raise funds for the benefit of the school.	Yes / No	
I am happy for the press to take and use images of my child.	Yes / No	
The school may give the press the first name (and first initial of surname) of my child for publishing with the child's photograph on the school and Trust's websites, in a newspaper or for captioning on television.	Yes / No	
I agree for an external company e.g. Tempest Photography, to take school photographs of my child for parental purchasing.	Yes / No	

Can we please remind you:

Use of Cameras and Digital Images (Parents/Carers) - 'THINK BEFORE WE POST'

Yealmpton Primary School are happy for parents and carers to take photos or videos at school events for personal use but please could we remind you that these images must not be distributed or put online unless they are only of your own children. This is to protect and safeguard all members of the community.

The Data Protection Act does not stop parents from taking images or videos at school events but you would breach it if you did not have the consent from other parents whose children might be captured in those photos or videos.

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

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

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

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

Acceptable Use Policy 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 the school 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, VLE , MS Teams, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will 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, I become aware of, to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE/ MS Teams) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking (School Facebook) sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
    - I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- I will not use a personal mobile phone device that I have brought into school for any activity that would be inappropriate in a school setting.
- When I use my mobile devices in school, I will follow the rules set out in this agreement, e.g., only during rest breaks away from children in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school/academy ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes
- I will ensure that my data is regularly backed up, in accordance with relevant school/academy policies.
- 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/academy 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/Academy/LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

- I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include: a warning, a suspension, referral to Governors/directors and/or the Local Authority and in the event of illegal activities the involvement of the police.

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

Staff/Volunteer Name: ..... Signed: .....

Date: .....

Acceptable Use Agreement for Community Users

This acceptable use agreement is intended to ensure:

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

Acceptable Use Agreement

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

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

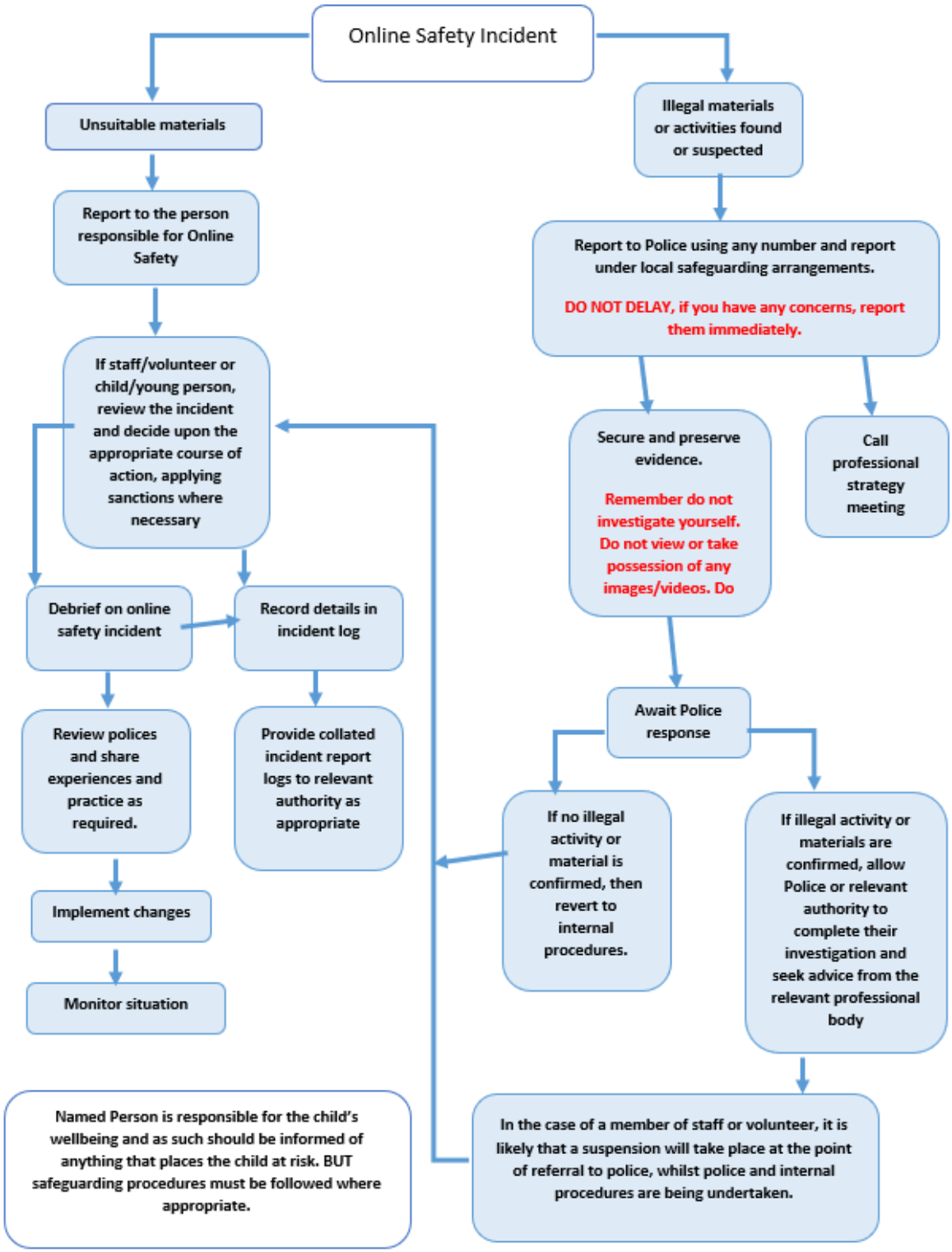
I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

As the school/academy is collecting personal data by issuing this form, it should inform community users about:

Who will have access to this form Senior Leaders /Admin	How this form will be destroyed. Stored electronically / deleted
Where this form will be stored. Office Secure Systems	How long this form will be stored for. Until community use ceases

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

Responding to incidents of misuse – flow chart



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

Group: .....

Date: .....

Reason for investigation: .....

.....

.....

Details of first reviewing person

Name: .....

Position: .....

Signature: .....

Details of second reviewing person

Name: .....

Position: .....

Signature: .....

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

.....

.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

Reporting Log

Group: .....

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

School Technical Security Policy (including filtering and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the *school infrastructure/network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of the WeST IT Team and Network Manager which manages the ICT service, it is the responsibility of the IT Team to carry out all the online safety measures that might otherwise be carried out by the *school and the team* is fully aware of the *school* online safety policy/acceptable use agreements.

Technical Security

Policy statements

The school working with WeST It Team will be responsible for ensuring that their 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 receive guidance and training and will be effective in carrying out their responsibilities:

- school technical systems will be managed in ways that ensure that the school meets recommended technical requirements (these may be outlined in the WeST Trust body technical/online safety policy)
- 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
- appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school/academy systems and data
- responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- all users will have clearly defined access rights to school technical systems. *Details of the access rights available to groups of users will be recorded by the network manager/technical staff/other person and will be reviewed, at least annually, by the online safety group.*
- users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- Trust Network Manager, Headteacher and Adminstrator 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 to ensure the school works within the Copyright Act.
- Mobile device security and management procedures are in place where mobile devices are allowed access to school systems.
- School, the Trust IT Team and 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.

- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system is in place (see appendix) for users to report any actual/potential technical incident to the online safety co-ordinator/network manager/technician (or other relevant person, as agreed)
- Permission is granted to the Adminstrator via Head teacher approval) for the provision of temporary access of "guests", (e.g. trainee teachers, supply teachers, visitors) onto the school/academy system
- There is minimal use of personal use that users (staff)are allowed on school devices that may be used out of school
- Staff use removable media (e.g. memory sticks/CDs/DVDs) by users on school devices and adhere to the WeST personal data policy
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see WeST Data Protection Policy

Password Security

A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and learning platform).

These statements apply to all users:

- All school networks and systems will be protected by secure passwords.
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the online safety group (or other group).
- All users (adults and pupils) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords must not be shared with anyone.
- All users will be provided with a username and password by the School Adminstrator or Trust IT Team .

Password requirements:

- Passwords should be long. Good practice highlights that passwords over 12 characters in length are considerably more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack.
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school.
- Passwords must not include names or any other personal information about the user that might be known by others
- Passwords must be changed on first login to the system

Technical Staff Teams

- Each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level.
- An administrator account password for the school/academy systems should also be kept in a secure place e.g. school administrator safe . This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account.
- Any digitally stored administrator passwords should be hashed using a suitable algorithm for storing passwords (e.g. Bcrypt or Scrypt). Message Digest algorithms such as MD5, SHA1, SHA256 etc. should not be used.
- *It is good practice that where passwords are used there is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password.*

- *Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated by an administrator who is easily accessible to users). Good practice is that the password generated by this change process should be system generated and only known to the user. This password should be temporary and the user should be forced to change their password on first login. The generated passwords should also be long and random.*
- *Where automatically generated passwords are not possible, then a good password generator should be used by the schooladmimistrator to provide the user with their initial password. There should be a process for the secure transmission of this password to limit knowledge to the password creator and the user. The password should be temporary and the user should be forced to change their password on the first login.*
- *Requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user*
- Suitable arrangements should be in place to provide visitors with appropriate access to systems which expires after use.
- In good practice, the account is "locked out" following six successive incorrect log-on attempts.
- Passwords shall not be displayed on screen, and shall be securely hashed when stored

Training/Awareness:

Members of staff will be made aware of the school password policy:

- at induction and through the school online safety policy and password security policy
- through the acceptable use agreement

Pupils will be made aware of the school's password policy:

- in lessons through the NC computing curriculum and through the acceptable use agreement

Audit/Monitoring/Reporting/Review:

The responsible person (Adminstrator and Online Safety Leader) will ensure that full records are kept of:

- User Ids and requests for password changes
- *User logons*
- *Security incidents related to this policy*

Filtering – Trust Network Manager

Introduction

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, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

DfE Keeping Learners Safe in Education requires schools to have "appropriate filtering". Guidance can be found on the UK Safer Internet Centre site.

Responsibilities Network Manager Check

The responsibility for the management of the school's filtering policy will be held by the Trust Network Manager. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must :

- be logged in change control logs
- be reported to a second responsible person
- *be reported to and authorised by a second responsible person prior to changes being made* (Network Manager)

- *or… be reported to a second responsible person* (Headteacher) *every X weeks/months in the form of an audit of the change control logs*
- *be reported to the Online Safety Group every X weeks/months in the form of an audit of the change control logs*

All users have a responsibility to report immediately to (insert title) 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.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- *The school maintains and supports the managed filtering service provided by the Internet Service Provider* –The Trust Network Manager and IT Team.
- *The school has provided enhanced/differentiated user-level filtering through the use of the* Network Manager *filtering programme. (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc.)*
- *In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher/Principal (or other nominated senior leader).*
- *Mobile devices that access the school/academy internet connection (whether school/academy or personal devices) will be subject to the same filtering standards as other devices on the school systems*
- *Any filtering issues should be reported immediately to the filtering provider.*
- *Requests from staff for sites to be removed from the filtered list will be considered by the technical staff* (Trust Network Manager and Turst IT Team.

Education/Training/Awareness

Pupils will be made aware of the importance of filtering systems through the online safety education programme following the Computing NC Curriculum. They will also be warned of the consequences of attempting to subvert the filtering system.

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

- the acceptable use agreement and online safety policy
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the acceptable use agreement and through online safety policy posted on the school website.

Changes to the Filtering System

In this section the school should provide a detailed explanation of:

- how, and to whom, users may request changes to the filtering (whether this is carried out in school or by an external filtering provider)
- the grounds on which they may be allowed or denied (schools may choose to allow access to some sites e.g. social networking sites for some users, at some times, or for a limited period of time. There should be strong educational reasons for changes that are agreed).
- how a second responsible person will be involved to provide checks and balances (preferably this will be at the time of request, but could be retrospectively through inspection of records/audit of logs)

- any audit/reporting system

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to (insert title) who will decide whether to make school level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the school online safety policy and the acceptable use agreement. *Staff will only implement the NC computing programme delivered through Kapow Computing Programmes of study . Topic research will be closely monitored by the staff.*

Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- the second responsible person (insert title)
- Safeguarding Team
- Online Safety Governor/Governors committee
- External Filtering provider/Local Authority/Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision. (The evidence might show a large number of requests to remove the filtering from sites – in which case schools might question whether their current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring/disciplinary action might be necessary).

Social Media Policy

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

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils are actively encouraged to find creative ways to use social media. However, there are

some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by *the school* its staff, parents, carers and children.

Scope

This policy is subject to the school's /academy's codes of conduct and acceptable use agreements.

This policy:

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

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

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

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

Digital communications with pupils/students are also considered. *Staff may use social media to communicate with learners via a school/academy social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.*

Organisational control

Roles & Responsibilities

- SLT
  - Facilitating training and guidance on Social Media use.
  - Developing and implementing the Social Media policy
  - Taking a lead role in investigating any reported incidents. Making an initial assessment when an incident is reported and involving appropriate staff external agencies as required.
  - Receive completed applications for Social Media accounts and Approve account creation

Administrator/Moderator

- Create the account following SLT approval
- Store account details, including passwords securely
- Be involved in monitoring and contributing to the account
- Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)

Staff

- Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
- Attending appropriate training
- Regularly monitoring, updating and managing content he/she has posted via school/academy accounts
- Adding an appropriate disclaimer to personal accounts when naming the school/academy

Process for creating new accounts

The school community considers which social media accounts will help them in their work, e.g. a Twitter account, or a Facebook page. Anyone wishing to create such an account must present a business case to the Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school/academy has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school/academy, including volunteers or parents.

Monitoring

School/academy accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school/academy social media account.

Behaviour

- The school/academy requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school/academy media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school/academy and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school/academy policies.
- The school/academy will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school/academy will deal with the matter internally. Where conduct is considered illegal, the school/academy will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of the school/academy, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Use of images

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

- Permission to use any photos or video recordings should be sought in line with the school's digital video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload pupil pictures online other than via school/academy owned social media accounts
- Staff should exercise their professional judgement about whether an image is appropriate to share on school/academy social media accounts. Pupils should be appropriately dressed, not be subject to ridicule and must not be on any school/academy list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

Staff

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school/academy, it must be made clear that the member of staff is not communicating on behalf of the school/academy 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/academy are outside the scope of this policy
- Where excessive personal use of social media in school/academy is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- *The school/academy permits reasonable and appropriate access to private social media sites.*

Pupil/Students

- Staff are not permitted to follow or engage with current or prior pupils of the school/academy on any personal social media network account.
- The school's education programme should enable the pupils to be safe and responsible users of social media.

Pupils are encouraged to comment or post appropriately about the school/academy. Any offensive or inappropriate comments will be resolved by the use of the school's/academy's behaviour policy

Parents/Carers

- If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
- The school/academy has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
- Parents/Carers are encouraged to comment or post appropriately about the school/academy. In the event of any offensive or inappropriate comments being made, the school/academy will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's/academy's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to this policy.

Managing your personal use of Social Media:

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

Managing school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible

The Don'ts

- Don't make comments, post content or link to materials that will bring the school/academy into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school/academy accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

Legislation

The legislative framework under which this online safety policy and guidance has been produced:

- Computer Misuse Act 1990
- Data Protection Act 1998
- The Data Protection Act 2018:
- Freedom of Information Act 2000
- Communications Act 2003
- Malicious Communications Act 1988
- Regulation of Investigatory Powers Act 2000
- Trade Marks Act 1994
- Copyright, Designs and Patents Act 1988
- Telecommunications Act 1984
- Criminal Justice & Public Order Act 1994
- Racial and Religious Hatred Act 2006
- Protection from Harassment Act 1997
- Protection of Children Act 1978
- Sexual Offences Act 2003
- Public Order Act 1986
- Obscene Publications Act 1959 and 1964
- Human Rights Act 1998
- The Education and Inspections Act 2006
- The Education and Inspections Act 2011
- The Protection of Freedoms Act 2012
- The School Information Regulations 2012
- Serious Crime Act 2015
- Criminal Justice and Courts Act 2015