Middleforth
C of E
Primary School

Online Safety Policy

Mission Statement
'Let Your Light Shine.'
Matthew 5:16

We seek to promote:
Faith
Resilience
Independence
Curiosity
Communication
Aspiration

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group made up of:
*   Headteacher & Senior Leaders
*   Online Safety Coordinator
*   Staff – including Teachers, Support Staff, Technical staff
*   Governors
*   Parents and Carers
*   Community users

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

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Headteacher	July 2021
The implementation of this Online Safety policy will be monitored by the:	Headteacher: Nicola Pilkington Online Safety Lead: David Swindells
Monitoring will take place at regular intervals	Once per academic year
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Once per academic year
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	July 2023
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LA Safeguarding Officer, LADO, Police

The school will monitor the impact of the policy using:
*   Logs of reported incidents
*   Monitoring logs of internet activity (including sites visited) / filtering
*   Internal monitoring data for network activity
*   Surveys / questionnaires of:

- Pupils
- Parents / carers
- Staff

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data in the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

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

Governors

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 Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:
- Regular meetings with the Online Safety Co-ordinator
- Attendance at Online Safety Group meetings
- Regular monitoring of online safety incident logs
- Regular monitoring of filtering / change control logs
- Reporting to relevant Governors meetings

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section "Responding to incidents of misuse" and relevant Local Authority disciplinary procedures).
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead
- Leads the Online Safety Group
- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with school technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering control logs
- Attends relevant meeting of Governors
- Reports regularly to Senior Leadership Team

Network Manager / Technical staff
The Network Manager / Technical Staff is responsible for ensuring:
- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher, Senior Leader; 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 current school Online Safety Policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the Headteacher, DSL; Online Safety Lead for investigation / action / sanction
- All digital communications with 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

> 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. Depending on the size or structure of the school this group may be 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 (or other relevant person, as above) with:
- The production / review / monitoring of the school Online Safety Policy / documents.
- Mapping and reviewing the online safety / digital literacy curricular provision – ensuring relevance, breadth and progression
- Monitoring network / internet / incident logs
- Consulting stakeholders – including parents / carers and the pupils about the online safety provision
- Monitoring improvement actions identified through use of the 360 degree safe self-review tool

Pupils
- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices, tablets and digital cameras
- They should also know and understand policies on the taking / use of images and on online bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

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 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 platforms and on-line pupil records

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

Policy Statements

Education – Pupils
Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. Online safety 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 and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / 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.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, 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, website, Learning Platform
- Parents / Carers workshops
- High profile events / campaigns e.g. Safer Internet Day

- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

The school will 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:
- 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
- Monthly e-safety newsletters

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:
- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events (e.g. from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Lead (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:
- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:
- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users in key stage 2 will be provided with a username and secure password by the online safety lead who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.

- The "master / administrator" passwords for the school ICT systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe)
- The School Business Manager, ICT Technician and Computing Coordinator 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 installations
- 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. This is currently Netsweeper through BT Lancashire, 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 school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different groups of users – staff / pupils etc)
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed). Staff will follow the safeguarding reporting system and report it to the DSL and online safety coordinator. Technical issues will also be reported to the ICT technician.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems. Specific accounts have been created for supply teachers, trainee teachers etc and temporary accounts can be created for specific visitors when needed.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices. Any files / programmes / apps are installed by the ICT technician.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Encrypted pen drives are used for sensitive data.

Mobile Technologies

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.

• The school Acceptable Use Agreements for staff, pupils and parents / carers will consider the use of mobile technologies
• The school allows:

	School devices		Personal Devices		
	School owned for single user	**School owned for multiple users**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	✓	✓	X	✓	✓
Full network access	✓	✓	X	X	X
Internet only			X	✓	✓

School owned / provided devices

• All teaching staff will be given teacher iPads to use to support teaching and learning. All teachers, teaching assistants and office staff have user logins to access the school network

• Devices can be used in school to support teaching and learning and can also be taken out of school for work purposes

• Personal use is not allowed

• All devices have access to the school internet and are filtered by the school filtering system

• The IT Technician is responsible for the management of devices, installation of apps and changing of settings and technical support. Devices are not regularly monitored but the school reserves the right to monitor as when they see feel it is needed. All staff have signed the Acceptable Use Policy

• All devices in school are filtered by BT Lancashire Services (BTLS) systems

• The devices have access have remote access to the school network, this is where work should be saved

• Devices are GDPR compliant through the use of passwords. These are school managed passwords

• Taking photos and storing them on devices is allowed for school purposes (for example: evidencing work, blogging). Use of images must follow school policies concerning the sharing, distribution and publication of those images.

• If a teacher leaves the school, the device is given back and wiped so it can be used by a different member of staff

• Devices are covered by school insurance for accidental damage, fire and theft. If it is lost by a member of staff then they will be responsible for replacing this

• Staff are given appropriate training to use the devices and are familiar with all the relevant policies regarding use of devices

Personal devices

• Staff and visitors are allowed to use personal mobile devices in school

• Mobile phones may only be used in designated areas. Guests devices will be given access specific to the task / activity

• Staff will not be allowed to use personal devices for school business except for school email accounts

• Devices will not have access to the networks. Staff can have access to the internet, visitors are given access through a 'guest' login

• No Technical support is available for personal devices

• The school reserves the right to take, examine and search users' devices in the case of misuse (England only) – n.b. this also included in the Behaviour Policy

• Taking / storage / use of images is forbidden on personal devices

• School takes no responsibility for the loss/damage or malfunction following access to the network. However, it is unlikely that any personal devices have access to the network

• Visitors will be informed about school requirements through the school handbook. Access to the school internet is only given upon request

• Pupils are educated about the safe and responsible use of mobile devices as part of Online Safety lessons.

Use of digital and video images

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

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images
- 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

Data Protection

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

The school must ensure that:
- It has a Data Protection Policy
- It has paid the appropriate fee to the Information Commissioner's Office (ICO)
- It has appointed a Data Protection Officer (DPO)
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified
- Data Protection Impact Assessments (DPIA) are carried out

- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller
- There are clear and understood data retention policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible
- Consideration has been given to the protection of personal data when accessed using any remote access solution
- All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities

Staff must ensure that they
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

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

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				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phone may be brought into school	✓						✓	
Use of mobile phone in lessons				✓				✓
Use of mobile phone in social times	✓							✓
Taking photos with mobile device/camera				✓				✓
Use of other personal mobile devices e.g. tablet or gaming device				✓				✓
Use of personal email in school, or on school network			✓					✓
Use of school email for personal emails				✓				✓
Use of messaging apps on school devices				✓				✓
Use of social media on school devices			✓					✓
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
- 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
- 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.
- Video communication between staff and pupils should clearly follow the guidelines set out in appendix 1

Social Media - Protecting Professional Identity

All schools**,** academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority / MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk
  School staff should ensure that:
- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

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

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

Personal Use
- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites. The school reserves the right to monitor devices when they feel it is appropriate.

Monitoring of Public Social Media
- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

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

Dealing with unsuitable / inappropriate activities
Some internet activity e.g. a
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:

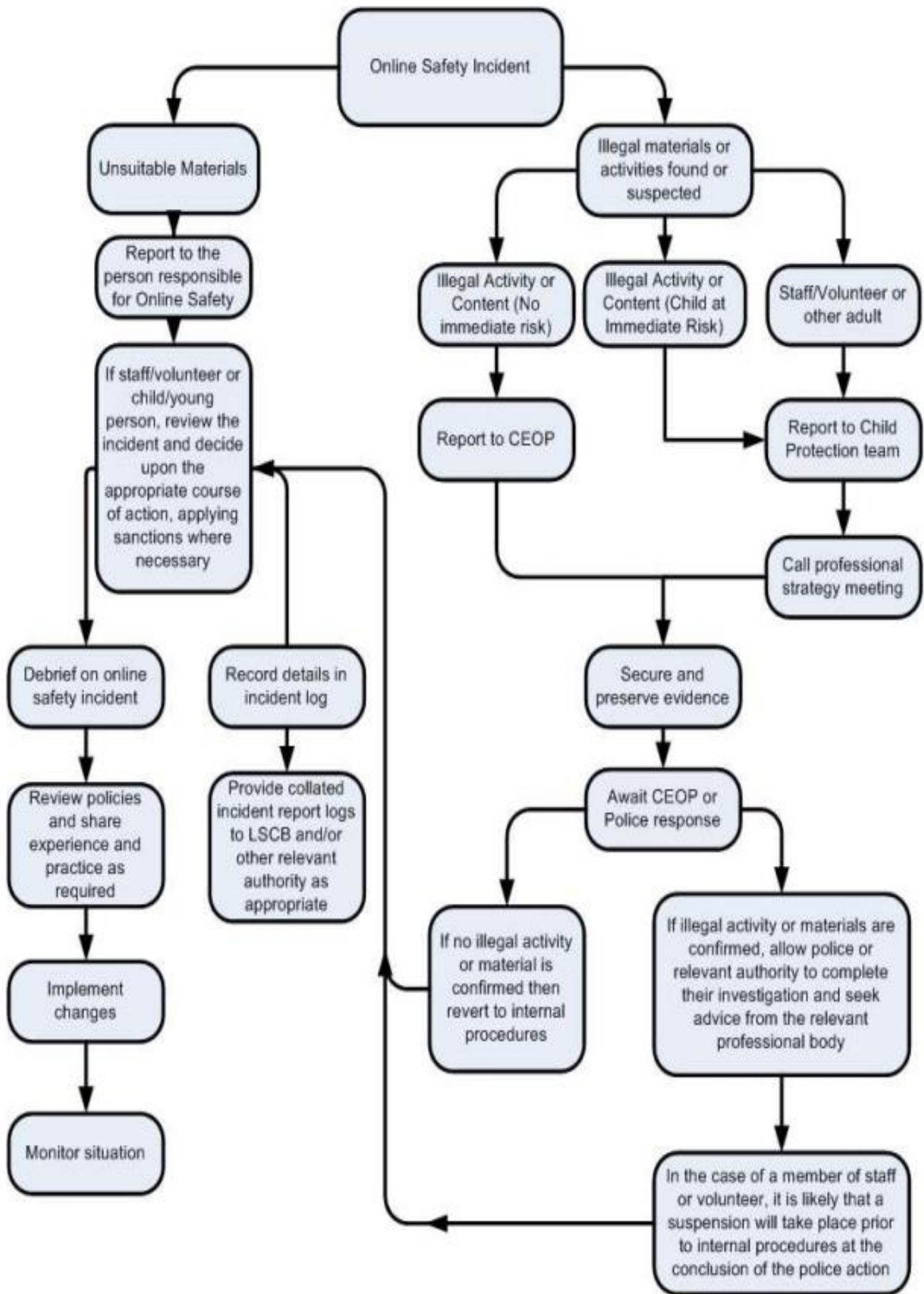| User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					✓
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					✓
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					✓
	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					✓
	Pornography				✓	
	Promotion of any kind of discrimination				✓	
	Threatening behaviour, including promotion of physical violence or mental harm				✓	
	Promotion of extremism or terrorism				✓	
	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				✓	
Using school systems to run a private business					✓	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					✓	

Activity	Col1	Col2	Col3	Col4	Col5
Infringing copyright				✓	
Creating or propagating computer viruses or other harmful files				✓	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				✓	
On-line gaming (educational)		✓			
On-line gaming (non-educational)				✓	
On-line gambling				✓	
On-line shopping / commerce		✓			
File sharing	✓				
Use of messaging apps		✓			
Use of social media		✓			
Use of video broadcasting e.g. Youtube	✓				

Responding to incidents of misuse

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

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

Online Safety Incident

Unsuitable Materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Review policies and share experience and practice as required

Implement changes

Monitor situation

Record details in incident log

Provide collated incident report logs to LSCB and/or other relevant authority as appropriate

Illegal materials or activities found or suspected

Illegal Activity or Content (No immediate risk)

Illegal Activity or Content (Child at Immediate Risk)

Staff/Volunteer or other adult

Report to CEOP

Report to Child Protection team

Call professional strategy meeting

Secure and preserve evidence

Await CEOP or Police response

If no illegal activity or material is confirmed then revert to internal procedures

If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

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: o Internal response or discipline procedures
  o Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
  o 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:
  o incidents of 'grooming' behaviour
  o the sending of obscene materials to a child
  o adult material which potentially breaches the Obscene Publications Act
  o criminally racist material promotion of terrorism or extremism
  o 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:

Students/Pupils Incidents	Actions/Sanctions								
	Refer to class teacher	Refer to Key Stage Leader	Refer to headteacher	Refer to police	Refer to technical support staff for action re filtering / security etc	Inform parents/carers	Removal of network/internet rights	warning	Further sanction e.g. detention or exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓					
Unauthorised use of non-educational sites during lessons	✓	✓	✓						
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	✓	✓	✓			✓			
Unauthorised / inappropriate use of social media / messaging apps / personal email	✓	✓	✓			✓			
Unauthorised downloading or uploading of files	✓	✓	✓						
Allowing others to access school network by sharing username and passwords	✓	✓	✓			✓			
Attempting to access or accessing the school network, using another student's / pupil's account	✓	✓	✓						
Attempting to access or accessing the school network, using the account of a member of staff	✓	✓	✓						
Corrupting or destroying the data of other users	✓	✓	✓						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓					✓	
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓			✓		✓	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school							✓	✓	
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓			✓		✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓	✓			✓			
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓			✓		✓	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓	✓			✓			

Staff Incidents	Refer to line manager	Refer to headteacher	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).		✔	✔	✔			✔	
Inappropriate personal use of the internet / social media / personal email		✔				✔		
Unauthorised downloading or uploading of files		✔				✔		
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		✔						
Careless use of personal data e.g. holding or transferring data in an insecure manner		✔						
Deliberate actions to breach data protection or network security rules		✔	✔			✔		✔
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✔	✔			✔		✔
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		✔	✔			✔		✔
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		✔	✔			✔		✔
Actions which could compromise the staff member's professional standing		✔	✔			✔		✔
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✔	✔			✔		✔
Using proxy sites or other means to subvert the school's filtering system		✔	✔			✔		✔
Accidentally accessing offensive or pornographic material and failing to report the incident		✔	✔		✔	✔		✔
Deliberately accessing or trying to access offensive or pornographic material		✔	✔				✔	✔

		✓				✓		
Breaching copyright or licensing regulations		✓					✓		
Continued infringements of the above, following previous warnings or sanctions			✓						✓

Signed:

Date:

Appendix 1

Video calling- Acceptable use Guidance
During the Covid-19 pandemic there will be reduced contact with children and video calling may be used to enable children to communicate with each other and their class teacher, should this take place then the following must be applied:

Parents

● Parental approval must be given before students may participate in online video conferences

● We will not hold 1:1 conferences with children

● Please identify a suitable location for your child to use for the video lesson for example a living room or dining area

● Parents should ensure that as far as possible distractions are removed and there is quiet

● Parents should familiarise themselves with the expectations on pupils set down in this guidance and ensure their child adheres to them

● Parents are responsible for ensuring that the privacy of other family members is maintained during video sessions

Teachers:

● Teachers will ensure that only students who have received parental approval participate in online video conferences.

● Teachers will only use school approved video conferencing platform (Zoom)

● Teachers will only use Seesaw to communicate with parents to gain permission.

● Teachers will contact parents and students through School email only Teachers will not use personal means of communication with parents, this will only take place through school approved means.

● Teachers will inform respective Senior Leadership Team staff of the regular scheduled online meetings.

● Teachers will keep a record of each Meet online (Date, time, length, attendees, topics)

● Online Meets will be kept to a reasonable time period, as devices and Internet may be in high demand at home

● Teachers will ensure students join the Meet with camera and microphones muted on entry.

● Teachers will ensure students abide by the School's Internet Acceptable Usage Policy at all times

● Teachers must conduct sessions in a professional manner, including being suitably attired during online sessions and ensuring they are broadcast from an appropriate location

● Where possible, video cameras should be used against a neutral background, with the light source directed towards the instructor's face

● At the end of a session the teacher must advise all students to leave the session and when all students have left the Meet, the teacher can then end the video conferencing session and terminate the meeting

Student

● Make sure you are in a suitable location; your device is charged (or plugged in) and

that you are suitably dressed prior to the beginning of each scheduled video conference.

● Check your camera and microphone are working prior to the start of the meeting.

● Remember to behave as you would in school and abide by the schools Internet Acceptable Usage Policy during sessions.

● Chat functions should be used to ask questions and to answer teacher questions.

● Please use chat functions responsibly and as directed by the teacher.

● Respect your teacher, your fellow learners and yourself by doing your best just as you would in class.

Appendix 2

Pupil acceptable use agreement
Dear Parent/Carer, Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access in our school. 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 users at risk.

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. Please read and discuss this agreement with your child and return the slip at the bottom of this page. If you have any concerns or would like a further explanation, please contact the teacher.

Acceptable Use Agreement

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

For my own personal safety:
- I understand that the school will monitor my use of the systems, devices and digital communications
- I will keep my username and password safe and secure - I will not share it, nor will I try to use any other person's username and password
- I will be aware of "stranger danger", where I am communicating on-line
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- I will immediately report any unpleasant or inappropriate material or message 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 act as I expect others to act towards 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 permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me:
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

● I will immediately report any damage or faults involving equipment or software, however this may have happened.

● I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).

● I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

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 cyber-bullying, use of images or personal information)

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, contact with parents and in the event of illegal activities involvement of the police.

Pupil Acceptable Use Agreement

Please complete your details below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement, If you do not sign and return the agreement, access will not be granted to school ICT systems. I have read and understood the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)

- I use my own equipment out of the school in a way that is related to me being a member of this school. e.g. communicating with other members of the school.

Name of pupil	
Class	
Date	
Signed pupil	
Signed parent/carer	

Appendix 3

Acceptable use agreement – 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 and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, 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/academy 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/academy 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.

Who will have access to this form: Headteacher, School Business manager and Online Safety Lead
Where this form will be stored: CSR
How long this form will be stored for: Length of policy
How this form will be destroyed : Secure deletion or shredding.

Appendix 4

<div align="center">

Staff acceptable use policy
September 2021

</div>

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/academy 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 students/pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE 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. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- 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) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students/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 local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will not use personal email addresses on the school ICT systems without express prior permission
- 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 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 policies
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School data 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 student/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.
- I will only use personal mobile phones and computing equipment in the agreed times and places detailed in the online safety policy, unless specific approval has been provided by the headteacher.

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: ………………………………………………………….