Policy Title:	**Online Safety - Whole School Policy**	
Date of Issue:	Autumn Term 2020	
Date of Review:	Spring Term 2021	
Author(s):	M Hodgeon / Online Safety Group	
Ratified by:	Governors	
Date:	19.11.2020	
Policy Committee Responsibility:	**Chair** W.Blundell	**Vice Chair** H.McCann
Outcome:	This Policy: details user responsibilities for Online Safety within Astley Park School, and is designed to help them understand their position	
Cross Reference:	Acceptable Use Policy Technical Security Policy Behaviour Policy Anti-Bullying Policy Child Protection and Safeguarding Policy Data Protection Policy Social Networking Policy Staff iPad Agreement	

EQUALITY AND DIVERSITY STATEMENT

Astley Park School is committed to the fair treatment of all in line with the Equality Act 2010. An equality impact assessment has been completed on this policy to ensure that it can be implemented consistently regardless of any protected characteristics and all will be treated with dignity and respect.

POLICY REVIEW

To ensure that this policy is relevant and up to date, comments and suggestions for additions or amendments are sought from users of this document. To contribute towards the process of review, please contact the author of the policy.

Table of Contents

Introduction

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by our Online Safety Group made up of:

- Governors
- Headteacher / Online Safety Lead
- DSL(s) / Online Safety Lead
- Strategic Lead ICT & Digital Transformation/ Online Safety Lead
- Send Support Manager
- Lead Practitioners
- Online Safety Curriculum Lead
- Parents
- Pupils (Digital Leaders)
- 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 Governing Body on:	12/06/2019
The implementation of this Online Safety policy will be monitored by the:	*Online Safety Group*
Monitoring will take place at regular intervals:	*Once a year*
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the DSL (which will include anonymous details of online safety incidents) at regular intervals:	*Once a year*
The Online Safety Policy will be reviewed every two years, 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:	22/05/2021
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer, LADO, Police, CSC*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Online Safety Group Meetings
- Surveys / questionnaires of
    - pupils
    - parents / carers
    - staff

Scope of the Policy

Deleted: ¶

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

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

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

Roles and Responsibilities

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

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:

- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meeting

Headteacher

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community.
- The Headteacher and (at least) another member of the Leadership and Management 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 is 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 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.

Designated Safeguarding Lead (DSL) / Online Safety Lead / Parent Carer Support Worker

- takes day to day responsibility for online safety issues
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of online safety incidents (via CPOMS/Suspicious Search Emails/Whisper) and creates a log of incidents to inform future online safety actions/developments.
- meets regularly with Online Safety/Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs
- Reports regularly to Leadership and Management Team / Governors
- attends Online Safety Group meetings

The DSL 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 / radicalisation
- online-bullying

Any incidents will be recorded via CPOMS and dealt with by the DSL.

Strategic Lead ICT & Digital Transformation / Online Safety Lead

The Strategic Lead for ICT /Online Safety Lead is responsible for ensuring:

- leads the Online Safety Group.
- 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 (BOOST) and advice for staff.
- attends Online Safety Group meetings.
- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority / Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see the school's Technical Security Policy for further details)
- 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 for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies
- ensure that the school's managed service provider is fully aware of the school Online Safety Policy and procedures

SEND Support Manager

- attends Online Safety Group meetings
- provides input into the Online Safety Policy
- provides advice and support to DSL for any Online Safety Interventions.

Online Safety Subject Lead

- attends Online Safety Group meetings
- Understanding curricular requirement
- Keeping up to date with current practice

- Curriculum content and Schemes of Work
- Monitoring of subject (Timetables, Evidence, Planning, Use of resources)
- Monitoring of progress Assessment (Data analysis, qualitative understanding)

Teaching and Support Staff, Supply and Volunteers

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 agreed to the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem via CPOMS 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
- liaise with the Online Safety Curriculum Lead for advice/guidance on the schools Online Safety Curriculum.

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. Minutes from the group will also be shared with the Governing Body.

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

- the production / review / monitoring of the school Online Safety Policy / documents.
- the production / review / monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.

- 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 and any improvements identified via the Online Safety Mark assessors report.
- play an active role in achieving/maintaining the school's Online Safety Mark.

Pupils

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

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, blogs, letters, website, school social media / 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' / online safety sections of the website / school social media
- their children's personal devices in the school (where this is allowed)

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the 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 / PSHCE / 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 online 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, pupils may need to research topics (eg 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 / Sharing our Learning activities
- Blogs, letters, school website/social media pages
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Dedicated Online Safety Page on school website
- Parent and Carer Support Manager / Strategic Lead ICT
- Reference to the relevant websites / publications e.g.
  https://internetmatters.org
  https://saferinternet.org.uk/advice-centre/parents-and-carers
  https://childnet.com/parents-and-carers

Education – The Wider Community

The school will provide opportunities for members of the wider 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
- Supporting other schools / groups to enhance their Online Safety provision by sharing good practice

Education & Training – Staff

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 DSL and Online Safety Lead will receive regular updates through attendance at external training events (eg 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 DSL / Online Safety Lead (or other nominated person) will provide advice / guidance / training to individuals as required.

Education & 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

If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the *school* Online Safety Policy / Acceptable Use Agreements. The school should also check their Local Authority / other relevant body policies on these technical issues.

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

For more details on Technical Security (including filtering and passwords) please refer to the school's **Technical Security Policy**.

Mobile Technologies (including BYOD)

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 platforms and other cloud-based services such as email and cloud storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. Mobile technologies should be used 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 any policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety curriculum.

- The school allows the use of:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Pupil owned**	**Staff owned**	**Visitor owned**
Allowed for use in school	*Yes*	*Yes*	*Yes*	*No[2]*	*Yes[2]*	*Yes[2]*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only (filtered)				*No*	*Yes*	*Yes*
No network access						

- The school Acceptable Use Agreements for staff and pupils considers the use of mobile technologies
- Staff iPads (School owned) require staff signing a Staff iPad Agreement.
- The school has provided technical solutions for the safe use of mobile technology for school devices/personal devices:
    - All school devices are controlled though the use of Mobile Device Management software
    - Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access)

[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.
[2] Personal devices in school can only be used in school under the conditions within AUP and Online Safety Policy.

- The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user. These may include; revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licenced software etc.
- All school devices are subject to routine monitoring
- Pro-active monitoring has been implemented to monitor activity

- When personal devices are permitted:
  - All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access
  - Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school
  - The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)
  - The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues
  - The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Passcodes or PINs should be set on personal devices to aid security
  - The school is not responsible for the day to day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues
- Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition;
  - Devices may not be used in tests or exams
  - Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements

- Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network
- Users are responsible for charging their own devices and for protecting and looking after their devices while in school
- Personal devices should be charged before being brought to school as the charging of personal devices is not permitted during the school day
- Devices must be in silent mode on the school site and on school buses
- School devices are provided to support learning. It is expected that pupils will bring devices to school as required.
- Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- The changing of settings (exceptions include personal settings such as font size, brightness, etc…) that would stop the device working as it was originally set up and intended to work is not permitted
- The software / apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps
- The school will ensure that school devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to pupils on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.
- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately
- Devices may be used in lessons in accordance with teacher direction
- Staff owned devices should not be used for personal purposes during teaching sessions.
- Printing from personal devices will not be possible

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded

themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press.
- 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/blog or social media, 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 solutions.
- All schools must have a Freedom of Information Procedure which sets out how it will deal with FOI requests (please refer to our Data Protection Policy for details).
- 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 device:

- 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 (below) 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			
Communication Technologies	Allowed /locked away in locker/ staff room	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed /locked away in locker	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	X	X			X			
Use of mobile phones in lessons				X				X
Use of mobile phones in social time		X						X
Taking photos on mobile phones / cameras				X				X
Use of other mobile devices e.g. tablets, gaming devices			X	X				X
Use of personal email addresses in school, or on school network				X				X
Use of school email for personal emails				X				X
Use of messaging apps				X				X
*Use of social media site				X				X
*Use of blogs			X	X			X	X

*official school social networking pages and class blogs only

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel

uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and pupils or parents / carers (email, social media, blogs, school texting service 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.
- Whole class / group email addresses may be used where appropriate and with guidance and monitoring from staff. Where appropriate pupils identified by the class teacher will be provided with individual school accounts / email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes please refer to the school's Social Networking Policy which sets out clear guidance for staff to manage risk and behaviour online.

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. online-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:

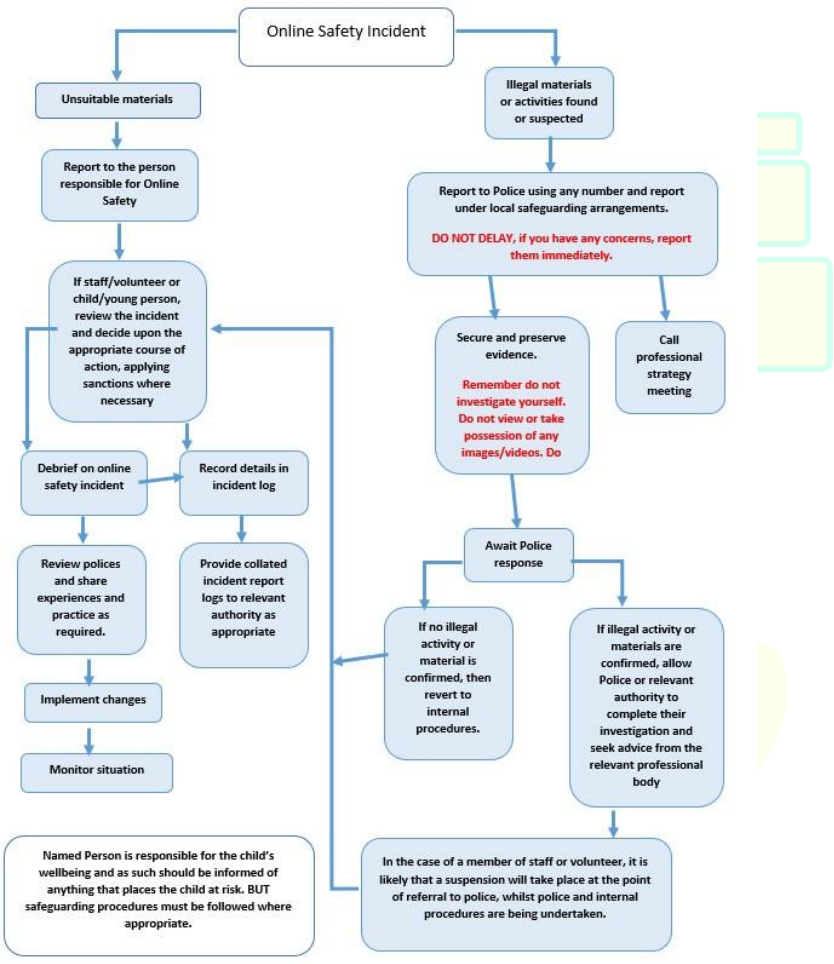
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child 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	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
Online gaming (educational)			X			
Online gaming (non-educational)					X	
Online gambling					X	
Personal online shopping / commerce					X	
Use of social media site (*official school social media pages only)				X	X	
Use of messaging apps					X	
Use of video broadcasting e.g. Facebook live, Youtube				X	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 website(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) 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 / national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- Isolate the computer/device 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	Record incident on CPOMS (Online Safeguarding)	Refer to DSL	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Targeted support/Consequence of continuation	Further sanction
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X		X	X	X	X
Unauthorised use of non-educational sites during lessons	X				X				
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device		X				X		X	
Unauthorised / inappropriate use of social media / messaging apps / personal email		X				X		X	
Unauthorised downloading or uploading of files	X	X			X	X		X	
Allowing others to access school network by sharing username and passwords	X	X			X	X		X	
Attempting to access or accessing the school network, using another pupil's account	X	X			X	X		X	

	Actions / Sanctions								
Pupils Incidents	Record incident on CPOMS (Online Safeguarding)	Refer to DSL	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Targeted support/Consequence of continuation	Further sanction
Attempting to access or accessing the school network, using the account of a member of staff	X	X			X	X		X	
Corrupting or destroying the data of other users	X	X			X	X		X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X				X		X	
Continued infringements of the above, following previous warnings or sanctions	X	X	X			X		X	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X			X		X	
Using proxy sites or other means to subvert the school's 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	
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	Refer to Local Authority / HR	Refer to Police	Refer to Strategic Lead for ICT for action re filtering /security	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X			X	X
Inappropriate personal use of the internet / social media / personal email		X			X	X	X	X
Unauthorised downloading or uploading of files		X				X	X	X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X			X	X	X	X
Careless use of personal data e.g. holding or transferring data in an insecure manner		X			X	X	X	X
Deliberate actions to breach data protection or network security rules		X			X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X				X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		X				X	X	X
Actions which could compromise the staff member's professional standing		X					X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X				X	X	X
Using proxy sites or other means to subvert the school's 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
Breaching copyright or licensing regulations		X				X	X	X

	Actions / Sanctions							
Staff Incidents	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Strategic Lead for ICT for action re filtering /security	Warning	Suspension	Disciplinary action
Continued infringements of the above, following previous warnings or sanctions		X					X	X