Wraxall Church of England Primary School

Online Safety Policy

Policy Approved by Governors:

Authorised for Issue: September 2022

To next be reviewed: September 2023

Our School Vision

Picture a school at the heart of the community, surrounded by nature and where the children can't wait to arrive in the morning because they know that they will experience the excitement and joy of learning.

Picture a school where the children are *inspired* to aim high and believe that their dreams are achievable because they will have developed the skills and knowledge needed. They have the confidence to challenge themselves because they know that their mistakes will only make them stronger. They will flourish and become all that they aspire to be.

Picture a school where the children are *nurtured* to be the best that they can be. They know that school is a safe and inclusive place because they have seen that all are welcomed and cared for. They will show compassion in all that they do and will make society a kinder place for all.

Picture a school where the children are celebrated for being unique individuals who together form a strong and united team. They become active and creative citizens who will **achieve** amazing things throughout their lives and develop a better future for all.

Picture Wraxall Church of England Primary School – *Inspiring, Nurturing, Achieving*

Our School Vision Statement takes as its starting point the following model developed by the Church of England and the Church in Wales:

'Recognising its historic foundation, the school will preserve and develop its religious character in accordance with the principles of the Church of England and in partnership with the Church at Parish and Diocesan level.'

The school vision also reflects the Church of England's Vision for Education and supports the promotion of Christian values. Our vision is based around elements of 'The Parable of the Sower'.

"The seeds sown in good soil" Mark 4: 13-20

In our school we follow our values to help us to show compassion towards others and our world. When we demonstrated our values, we are helping our school to grow and flourish and enabling our community to live "life in all its fullness" John 10:10

Our School Christian Values

Our School's Christian Values are demonstrated in all that we do and say

   *Compassion * Responsibility * Respect * Perseverance * Friendship * Honesty * Courage

Wraxall Primary School
Online Safety Policy
Incorporating Mobile Devices & Search and Delete (Confiscate)

This policy should be read alongside the Safeguarding Policy and the Covid-19 School Closure Arrangements for Safeguarding and Child Protection safeguarding policy addendum (which includes MS Teams and Live Streaming).

Development, monitoring and review of this policy

This Online Safety policy has been developed by a group of Wraxall school teachers and governors made up of:

- Headteacher - Amy Townsend
- Online Safety Coordinator – Victoria Sheppard/Sinead Cope
- Safeguarding Governor – Hazel Mallett
- Health and Safety Governor – Hazel Mallett
- Pupils – E-safety committee members – three UKS2 pupils

Schedule for Development, Monitoring & Review

This Online Safety policy was approved by the Governing Body on	September 2022
The implementation of this Online Safety policy will be monitored by the:	e-safety committee
Monitoring will take place at regular intervals:	Annually
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:	Annually
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:	September 2023
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Somerset Multi Agency Safeguarding Hub (Southern MASH), Police, SWGFL, LADO, LSP Safeguarding Team dependant on the specifics of the incident

The school will monitor the impact of the policy using:

- Logs of reported incidents in the Online Safety Folder
- CPOMS

- Monitoring logs of internet activity (including sites visited) / filtering available through school technician
- Annual 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 ICT 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 cyber-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 . This is combined with that of the Child Protection/Safeguarding Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- reporting to relevant Governors / Board / Committee / meeting

- Monitoring of filtering/change control logs

Headteacher:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *LSP MAT* 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.
- The Headteacher will receive regular monitoring reports from the Online Safety Co-ordinator.

Online Safety Coordinator:

- 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 / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the LSP MAT (and Local Authority as necessary)
- 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/change control logs.
- attends relevant meeting of Governors
- reports regularly to Senior Leadership Team

Technical staff:

LSP has a managed ICT Service provided by 2iT (outside contractor).

The 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 LSP MAT 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 schools filtering system is working effectively and that the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that the use of the network and internet is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction
- that monitoring software or 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/ 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/Deputy 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
- cyber-bullying

Online Safety Group

The Online Safety Group provides a consultative group that has 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 with:

- the production / review / monitoring of the school Online Safety Policy
- the production/review/monitoring of the school filtering policy (if possible and 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 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 Policy 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 cyber-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, 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
- their children's personal devices in the school (permission MUST be requested from the Headteacher in advance of these being on school site).

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 students to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision and in collaboration with the Prevent Duty. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for:
> *"a carefully sequenced RSHE curriculum, based on the Department for Education's (DfE's) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of 'nudes'.."*

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/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 Policy 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 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 on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- *Curriculum activities*
- *Letters, newsletters, web site*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites / publications*
  e.g. www.swgfl.org.uk
  www.saferinternet.org.uk

www.childnet.com/parents-and-carers

Education – The Wider Community

The school will provide opportunities for members of the community to gain from the schools online safety knowledge and experience. This may be offered through the following:

- *Providing family learning courses in use of new digital technologies, digital literacy and online safety*
- *Online safety messages targeted towards grandparents and other relatives as well as parents.*
- *The school website will provide online safety information for the wider community*
- *Supporting community groups e.g. Church playgroup*
- *Sharing online safety expertise/good practice with other local schools*

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 schools Online Safety Policy and Acceptable Use Policy Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The 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/online webinars e.g. from NOS
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings.
- The Online Safety Coordinator 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 / academy training / information sessions for staff or parents (this may include attendance at assemblies / lessons).
- Membership and access of NOS (if available)

Technical – infrastructure / equipment, filtering and monitoring

LSP MAT has a manages ICT service provided by 2iT, an external contractor.

The school will be responsible for ensuring that the schools 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:

- An Acceptable Use Policy Agreement is in place for all staff, governors, supply teachers, trainee teachers and other volunteers, parents and children.
- 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, at KS2 and above, will be provided with a username and secure password by the technical staff, who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every year.
- The administrator passwords for the school ICT system, 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 (eg school safe)
- ICT technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users**.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- School technical staff monitor the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person.
- 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. Temporary access for guests is through guest wifi and not school wifi.

- The Acceptable Use Policy Agreement is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- The Staff and Volunteer Acceptable Use Policy Agreement is in place that explains staff responsibilities when downloading executable files and installing programmes on school devices.
- The Staff and Volunteer and Community User Acceptable Use Policy Agreements are in place which explains the use of removable media in school (e.g. memory sticks) by users on school devices.

Mobile Technologies (including BYOD)

The DfE guidance "Keeping Children Safe in Education" states:
> "The school or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share

pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, 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 learning platform and other cloud-based services such as e-mail and data storage.

All users should understand that the primary purpose of the use of 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 those for safeguarding, behaviour, anti-bullying, acceptable use, 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.

In preparing a mobile technologies policy the school should consider possible issues and risks. These may include:

- security risks in allowing connections to your school network
- filtering of personal devices
- breakages and insurance
- access to devices for all learners
- avoiding potential classroom distraction
- network connection speeds, types of devices
- charging facilities
- total cost of ownership.

A range of mobile technology strategies is possible. However, these need to be thoroughly researched, risk assessed and aligned with existing policy prior to implementation. A more detailed mobile technologies policy template can be found in the Appendix.

The school acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.
- The school allows:
  o The School Wifi network code will not be shared with non-school owned devices. A Guest wi-fi network is permissible for non-school owned devices.
  o The school wifi network code is available only from the Headteacher and is stored securely. It can only be accessed from the IT support team with the permission of the Headteacher or in their absence the Deputy Headteacher.

	School Devices		Personal Devices		
	School owned for single user	**School owned for multiple users**	**Student owned with permission**	**Staff owned**	**Visitor owned**
Allowed in school	Yes	Yes	No*	Yes**	Yes*

Full network access	Yes	Yes			
Internet access	Yes	Yes			With HT permission
No network access			No network access	No network access	No network access

*To be kept in school office. Permission must be given from Headteacher for visitors to have online devices in school in locations other than the school office. **Staff phones to be kept in lockers in the staffroom, Headteacher's office or the main school office unless the prior permission is given by the Headteacher eg. Emergency use on school trips.

- **The school has provided technical solutions for the safe use of mobile technology for school devices/personal devices (delete/amend as appropriate):**
  - o **All school devices are controlled though the use of Mobile Device Management software**
  - o **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)**
  - o **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**
  - o **For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted**
  - o **Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user**.
  - o *All school devices are subject to routine monitoring*
  - o *Pro-active monitoring has been implemented to monitor activity*

- *When personal devices are permitted:*
  - o *All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access*
  - o *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*
  - o *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)*
  - o *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*
  - o *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. Pass-codes or PINs should be set on personal devices to aid security*
  - o *The school is not responsible for the day to day maintenance or upkeep of the users 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 the school**
  - **Personal devices should be charged before being brought to the school as the charging of personal devices is not permitted during the school day**
  - **Devices must be in silent mode on the school site and on school buses**
  - **School devices are provided to support learning. It is expected that learners will bring devices to the school as required.**
  - **Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.**
  - **The changing of settings (exceptions include personal settings such as font size, brightness, etc…) that would stop the device working as it was originally set up and intended to work is not permitted**
  - **The software/apps originally installed by the school must remain on the school owned device in usable condition and be 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 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 learners 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, unless in exceptional circumstances*
  - *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 onlinebullying 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.

- 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 photographs/work can only be published with the permission of the pupil and parents or carers.

Data Protection

See Data Protection Policy

Communications

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

Staff & other adults	*Students / Pupils*

Communication Technologies

	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school / academy	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		
Use of personal email addresses in school / academy , or on school / academy network		X						X
Use of school / academy email for personal emails		X						X
Use of messaging apps				X				X
Use of social media				X				X
Use of blogs				X				X

X = Where no children are present and no names or other personal information is included and for school use. . Eg. a display of unnamed work for a school newsletter. Only with the express permission of the Headteacher. The photograph must be supervised by the Headteacher **and** with the additional supervision of another member of the SLT (either the Deputy Headteacher or Office Manager).

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

- The official school email service may be regarded as safe and secure. 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 DSL/DDSL, who will then inform the online safety coordinator, the receipt of any communication that makes them feel uncomfortable is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or social media must NOT be used for these communications.
- 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

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools, 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 onlinebullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school, MAT* or local authority 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 MAT 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 / academy disciplinary procedures

Personal Use:

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

- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

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 senior risk officer and Online Safety Group to ensure compliance with the school policies.

Dealing with Unsuitable / inappropriate activities

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

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal

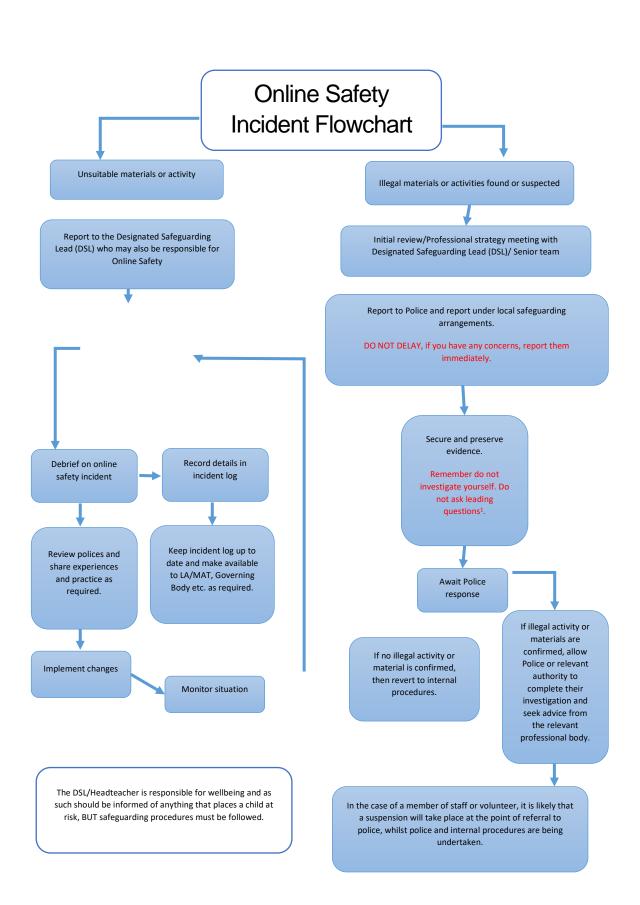| Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:					
Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 and other associated legislation					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 / academy				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	
On-line gaming (educational)		X			
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce		X			
File sharing		X			
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting e.g. Youtube		X			

Responding to incidents of misuse

This guidance is intended for use when staff members 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 for responding to online safety incidents and report immediately to the police.

Online Safety
Incident Flowchart

Unsuitable materials or activity

Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety

Illegal materials or activities found or suspected

Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team

Report to Police and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not ask leading questions[1].

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.

Implement changes

Monitor situation

Await Police response

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

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

The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
    - Police involvement and/or action

- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - Offences under the Computer Misuse Act (See User Actions Chart Above)
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School / Academy 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 / Pupil Incidents	Actions / Sanctions
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 / academy network by sharing username and passwords	Refer to class teacher
Attempting to access or accessing the school / academy network, using another student's / pupil's account	Refer to SLT
Attempting to access or accessing the school / academy network, using the account of a member of staff	Refer to Headteacher Refer to Police
Corrupting or destroying the data of other users	Refer to technical support staff for action re filtering / security etc.
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	Inform parents / carers
Continued infringements of the above, following previous warnings or sanctions	Removal of network / internet access rights
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school	Warning Further sanction eg detention / exclusion
Using proxy sites or other means to subvert the school's / academy'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 / Adult User Incidents	Actions / Sanctions
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	Refer to line manager
	Refer to Headteacher
Inappropriate personal use of the internet / social media / personal email	Refer to Local Authority / HR
	Refer to Police
Unauthorised downloading or uploading of files	Refer to Technical Support Staff for action re filtering etc.
Allowing others to access school network by sharing username and passwords or attempting to access or	Warning

	Suspension
accessing the school network, using another person's account	Disciplinary action
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 students / pupils	
Actions which could compromise the staff member's professional standing	
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	
Using proxy sites or other means to subvert the school's / academy'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	

In the event of such an incident occurring, a written record would be made describing both the incident and the action taken, together with rationale appropriate. This record will be retained within the individual's personal file and e-safety incident log and safeguarding file as appropriate.

PASSWORD POLICY

Introduction

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:
• users can only access data to which they have right of access
• no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
• access to personal data is securely controlled in line with the school's personal data policy
• logs are maintained of access by users and of their actions whilst using the system

Responsibilities

The management of the password security policy will be the responsibility of the online safety coordinator, ICT technician (2iT)and SLT.

Password Security

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

Policy Statements:

- **These statements apply to all users.**
- **All school networks and systems will be protected by secure passwords.**
- **All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by 2iT (The Network Manager) and will be reviewed, at least annually, by the online safety group of adults.**
- **All users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.**
- **Passwords must not be shared with anyone.**
- **All users will be provided with a username and password** by 2iT directly who will keep an up to date record of users and their usernames or via. the Headteacher/Deputy headteacher and the user will be told to change their password once they have logged in.

Password requirements:

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

All adults and pupils in Key Stage 2 will have responsibility for the security of their username and password. Adults and pupils in KS2 must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. In Key Stage 1, class logins will be used but monitored by the relevant class teachers, with any concerns being passed on to the online safety coordinator.

Passwords for new users and replacement passwords for existing users will be allocated by the ICT Technician. All users at KS2 will be provided with a username and password by the ICT Technician (2iT) who will keep an up to date record of users and their usernames.
The following rules apply to the use of passwords:
• Never reveal your password to anyone
• Do not use any part of your username within the password
• Never write your password down or store them where they are left open
• Passwords shall not be displayed on screen, and shall be securely hashed
• Requests for password changes should be made in person to the online safety coordinator or 2iT IT Technician, ensuring that the new password can only be passed to the genuine user.

The following rules apply to the use of passwords for adults:
•
• Adult passwords should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character and number.
Computers and laptops MUST be screen locked when leaving a room.
The "administrator" passwords for the school ICT system, used by the ICT technician and online safety coordinator must also be available to the Headteacher or other nominated senior leader and kept in a secure place.

Training / Awareness

Members of staff will be made aware of the school's password policy:
• At induction.
• Through this policy.
• Through the Acceptable Use Policy Statement.

Pupils / students will be made aware of the school's password policy:
• In computing, PSHE or E-safety lessons.
• Through the Acceptable Internet Use Statement.

MOBILE PHONE POLICY

(Including Mobile Devices)

Introduction

This policy outlines the appropriate use of mobile phones on our school site.

The widespread ownership of mobile phones among young people requires that school administrators, teachers, pupils, and parents take steps to ensure that mobile phones are used responsibly at school.

Pupils

We recognise that many pupils and their families own a mobile phone. We also recognise that some parents/guardians request that their child/ren bring a mobile phone to school for safety/security reasons.

Our core business of teaching and learning needs to be conducted in an environment free from unnecessary distractions or disruptions. Therefore the school strongly discourages the possession of mobile phones in school by pupils. There are no reasons why a pupil needs to have in their possession, or use, a mobile phone during the school day. Parents are reminded that in cases of emergency the school office remains a vital and appropriate point of contact. This ensures your child is reached quickly and assisted in any appropriate way.

The school is prepared to allow mobile phones on the premises but only within the parameters of the policy as stated below.

Responsibility

It is the responsibility of pupils who bring mobile phones to school to abide by the guidelines outlined in this document.

- The decision to provide a mobile phone to their child/ren should be made by parents or guardians.
- Parents should be aware if their child/ren takes a mobile phone to school.
- Permission to have a mobile phone at school, while under the school's supervision, is dependent on parent/guardian permission in the form of a signed copy of this policy. Parents/guardians may revoke approval at any time.
- Pupils must hand the mobile phone/ device in to the school office upon arrival and collect it at the end of the day.

Sanctions

Pupils who fail to follow these guidelines will have their phones confiscated. The phone will only be handed back to the parent/guardian. The school may revoke the right for pupils to bring a mobile phone onto the school grounds.

It should be noted that it is a criminal offence to use a mobile phone to menace, harass or offend another person. The school may consider it appropriate to involve the police.

Child's Name _____

Parent/ Guardian signature _____

Date_____

Staff

It is the responsibility of staff who bring mobile phones to school to abide by the guidelines outlined in this document.

- During teaching time, mobile phones will be stored in lockers in the staffroom or the school office if awaiting an important phone call (with the Headteacher's permission).
- Mobile phone use is not permitted during teaching time, while on playground duty and during meetings, unless permission is given by the headteacher.

- Mobile phones can only be used in the designated zones during school hours.
  These zones are:

  School office

  Staff room – when children are not present

  Headteacher's office.
- Any individual bringing a personal device into the setting must ensure that it contains no inappropriate or illegal content.
- Any breach of these procedures could lead to the E-safety committee being informed and consequently disciplinary action according to the schools procedures.

Visitors

All visitors/volunteers/contractors must hand their mobile phone/online device in to the school office for safekeeping upon arrival to the school site. Student teachers will be given a locker space in the staffroom to store their phone in. An exception maybe arranged with the headteacher depending on the reason for the visit i.e. ICT technician.

School Online Safety Policy Template: Electronic Devices - Searching Screening and Confiscation

The Education Act 2012, the basis of this template, sets out what the law is presumed to be, based on prior legal and educational knowledge, and common sense. Rights and responsibilities regarding physical contact and personal data are still evolving rapidly. So too are social, entertainment and educational technologies and the skills necessary to use them safely and prudently. This is particularly so where those who are under 18 are involved.

No existing law or policy can fully insulate anyone from the risk involved in searching for, access to or deletion of the personal data of others. Anyone refraining from any such search, access or deletion when hindsight shows circumstances merit such actions may however be at significant risk and may put seriously at risk the wellbeing of children entrusted to their care.

Introduction

The changing face of information technologies and ever-increasing learner use of these technologies has meant that the Education Acts were updated to keep pace. Part 2 of the Education Act 2011 (Discipline) introduced changes to the powers afforded to schools by statute to search learners in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

The particular changes we deal with here are the added power to screen, confiscate and search for items 'banned under the school rules' and the power to 'delete data' stored on confiscated electronic devices.

Items banned under the school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).

An item banned by the school rules may only be searched for under these new powers if it has been identified in the school rules as an item that can be searched for. It is therefore important that there is a school policy which sets out clearly and unambiguously the items which:

- are banned under the school rules; and
- are banned AND can be searched for by authorised school staff

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question relates to an offence and/or may be used to cause harm, to disrupt teaching or could break the school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, **if they think there is a good reason to do so** (see later section)

The Headteacher must publicise the school behaviour policy, in writing, to staff, parents/carers and learners at least once a year. (There should therefore be clear links between the search etc. policy and the behaviour policy).

DfE advice on these sections of the Education Act 2011 can be found in the document: "Screening, searching and confiscation – Advice for schools" (**updated July 2022**)

It is recommended that Headteachers (and, at the least, one other senior leader) should be familiar with this guidance.

The DfE Guidance – "Behaviour in Schools" was updated in July 2022 and refers to behaviour online:

> "The way in which pupils relate to one another online can have a significant impact on the culture at school. Negative interactions online can damage the school's culture and can lead to school feeling like an unsafe place. Behaviour issues online can be very difficult to manage given issues of anonymity, and online incidents occur both on and off the school premises. Schools should be clear that even though the online space differs in many ways, the same standards of behaviour are expected online as apply offline, and that everyone should be treated with kindness, respect and dignity.
>
> Inappropriate online behaviour including bullying, the use of inappropriate language, the soliciting and sharing of nude or semi-nude images and videos and sexual harassment should be addressed in accordance with the same principles as offline behaviour, including following the child protection policy and speaking to the designated safeguarding lead (or deputy) when an incident raises a safeguarding concern.
>
> Many online behaviour incidents amongst young people occur outside the school day and off the school premises. Parents are responsible for this behaviour. However, often incidents that occur online will affect the school culture. Schools should have the confidence to sanction pupils when their behaviour online poses a threat or causes harm to another pupil, and/or could have repercussions for the orderly running of the school, when the pupil is identifiable as a member of the school or if the behaviour could adversely affect the reputation of the school.
>
> Headteachers should decide if **mobile phones** can be used during the school day. Many pupils, especially as they get older, will have one of their own. Allowing access to mobiles in school introduces complexity and risks, including distraction, disruption, bullying and abuse, and can be a detriment to learning. Headteachers should consider restricting or prohibiting mobile phones to reduce these risks.
>
> If headteachers decide not to impose any restrictions on mobile phones, they should have a clear plan to mitigate the risks of allowing access to phones. This plan, as part of the school's behaviour policy, should outline the approach to mobile phones and be reiterated to all pupils, staff and parents throughout the school year. Headteachers should ensure it is consistently and fairly applied."

A new Keeping Children Safe in Education guidance document is in force from September 2022. Schools should be aware of new guidance concerning **Harmful Sexual Behaviour** (see policy template in these appendices):

"Following any report of child-on-child sexual violence or sexual harassment offline or online, schools should follow the general safeguarding principles set out in Keeping children safe in education (KCSIE) - especially Part 5. The designated safeguarding lead (or deputy) is the most appropriate person to advise on the school's initial response. Each incident should be considered on a case-by-case basis.

Schools should be clear in every aspect of their culture that sexual violence and sexual harassment are never acceptable, will not be tolerated and that pupils whose behaviour falls below expectations will be sanctioned. Schools should make clear to all staff the importance of challenging all inappropriate language and behaviour between pupils. Schools should refer to the Respectful School Communities toolkit for advice on creating a culture in which sexual harassment of all kinds is treated as unacceptable."

Relevant legislation:
- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990

This is not a full list of Acts involved in the formation of this advice. Further information about relevant legislation can be found via the above link to the DfE advice document.

Responsibilities

The Headteacher is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will normally be taken to Governors for approval. The Headteacher will need to authorise those staff who are allowed to carry out searches.

This policy has been written by and will be reviewed by: Headteacher, Online Safety Lead, DSL/DDSL, Governors including Safeguarding Governor/

The Headteacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data/files on those devices: Headteacher, Deputy Headteacher, DSL and/or DDSL

The Headteacher may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

Members of staff (other than Security Staff) cannot be required to carry out such searches. They can each choose whether or not they wish to be an authorised member of staff.

Training/Awareness

It is essential that all staff should be made aware of and should implement the school's policy.

Members of staff should be made aware of the school's policy on "Electronic devices – searching, confiscation and deletion":

- at induction
- at regular updating sessions on the school's online safety policy

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data/files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Policy Statements
Search:

The school **Behaviour Policy** refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data/files on those devices.

Learners are not allowed to bring mobile phones or other personal electronic devices to school or use them in the school. If they bring them onto school site they must have their parents written permission on the mobile permissions form and their phone must be handed into the school office on arrival at school for safe keeping and not collected until the end of the school day.

The sanctions for breaking these can be found 'mobile phone policy' section of this policy.

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent - Authorised staff may search with the learner's consent for any item
- Searching without consent - Authorised staff may only search without the learner's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for

In carrying out the search:

The authorised member of staff must have reasonable grounds for suspecting that a *learner* is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for. (Whether there are 'reasonable grounds' is a matter decided on by reference to the circumstances witnessed by, or reported to, someone who is authorised and who exercises properly informed professional judgment and has received appropriate training).

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone/personal electronic device before carrying out a search. (The powers included in the Education Act do not extend to devices owned (or mislaid) by other parties e.g. a visiting parent or contractor, only to devices in the possession of learners.)

The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the learner being searched.

The authorised member of staff carrying out the search must be the same gender as the *learner* being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the *learner* being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a learner of the opposite gender including without a witness present, but **only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.**

Extent of the search:
The person conducting the search may not require the learner to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

'Possessions' means any goods over which the learner has or appears to have control – this includes desks, lockers and bags. (schools will need to take account of their normal policies regarding religious garments/headwear and may wish to refer to it in this policy)

A learner's possessions can only be searched in the presence of the learner and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Electronic devices

The DfE guidance – Searching, Screening and Confiscation received significant updates in July 2022 and now states:

- Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.
- As with all prohibited items, staff should first consider the appropriate safeguarding response if they find images, data or files on an electronic device that they reasonably suspect are likely to put a person at risk
- Staff may examine any data or files on an electronic device they have confiscated as a result of a search .. if there is good reason to do so (defined earlier in the guidance as)
    - poses a risk to staff or pupils;

- o is prohibited, or identified in the school rules for which a search can be made or
- o is evidence in relation to an offence.
- If the member of staff conducting the search suspects they may find an indecent image of a child (sometimes known as nude or semi-nude images), the member of staff should never intentionally view the image, and must never copy, print, share, store or save such images. When an incident might involve an indecent image of a child and/or video, the member of staff should confiscate the device, avoid looking at the device and refer the incident to the designated safeguarding lead (or deputy) as the most appropriate person to advise on the school's response. Handling such reports or concerns can be especially complicated and schools should follow the principles as set out in Keeping children safe in education. The UK Council for Internet Safety also provides the following guidance to support school staff and designated safeguarding leads: Sharing nudes and semi-nudes: advice for education settings working with children and young people.
- If a member of staff finds any image, data or file that they suspect might constitute a specified offence, then they must be delivered to the police as soon as is reasonably practicable.
- In exceptional circumstances members of staff may dispose of the image or data if there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files, the member of staff must have regard to the following guidance issued by the Secretary of State
  - o In determining whether there is a 'good reason' to examine the data or files, the member of staff should reasonably suspect that the data or file on the device has been, or could be used, to cause harm, undermine the safe environment of the school and disrupt teaching, or be used to commit an offence.
  - o In determining whether there is a 'good reason' to erase any data or files from the device, the member of staff should consider whether the material found may constitute evidence relating to a suspected offence. In those instances, the data or files should not be deleted, and the device must be handed to the police as soon as it is reasonably practicable. If the data or files are not suspected to be evidence in relation to an offence, a member of staff may delete the data or files if the continued existence of the data or file is likely to continue to cause harm to any person and the pupil and/or the parent refuses to delete the data or files themselves

The examination of the data/files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge. It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage.

Members of staff may require support in judging whether the material is inappropriate or illegal. One or more Senior Leaders should receive additional training to assist with these decisions. Care should be taken not to delete material that might be required in a potential criminal investigation.

The school should also consider their duty of care responsibility in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such

material can be most upsetting. There should be arrangements in place to support such staff. The school may wish to add further detail about these arrangements.

Further guidance on reporting the incident to the police and the preservation of evidence can be found in the SWGfL flow chart in the main School Template Policies document. Local authorities/local safeguarding partnerships may also have further guidance, specific to their area.

A record should be kept of the reasons for the deletion of data/files. (DfE guidance states and other legal advice recommends that there is no legal reason to do this, best practice suggests that the school can refer to relevant documentation created at the time of any search or data deletion in the event of a learner, parental or other interested party complaint or legal challenge. Records will also help the school to review online safety incidents, learn from what has happened and adapt and report on application of policies as necessary).

Care of Confiscated Devices
School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage/loss of such devices (particularly given the possible high value of some of these devices).

The school may wish to add a disclaimer to the relevant section of the Behaviour Policy which may assist in covering the school against damage/loss claims.

Audit/Monitoring/Reporting/Review
The responsible person, Headteacher and Deputy Headteacher, will ensure that full records are kept of incidents involving the searching for and of electronic devices and the deletion of data/files.

These records will be reviewed by Safeguarding and Online Safety Governor at regular intervals (at least once a year).

This policy will be reviewed by the head teacher and governors annually and in response to changes in guidance and evidence gained from the records.

The school is required is publish its Behaviour Policy to parents annually (including on its website) – the Behaviour Policy should be cross referenced with this policy on search and deletion. DfE guidance can be found at: https://www.gov.uk/government/publications/searching-screening-and-confiscation

Policy Statements
All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the online safety coordinator and will be reviewed, at least annually, by the E-safety Committee.

Audit / Monitoring / Reporting / Review
The Online safety coordinator/ Technician will ensure that full records are kept of:
• User IDs
• Security incidents related to this policy.

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption. Local Authority Auditors also have the right of access to passwords for audit investigation purposes.

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

These records will be reviewed by the E-safety Committee at regular intervals with a minimum of once a year.

The policy will be reviewed annually in response to changes in guidance and evidence gained from the logs.

Declarations

This E-safety policy was checked by the:

Head Teacher: ………………Amy Townsend......................................on 02 / 09 / 2022

Online safety coordinator……………………………………………………on   ……. / ……. / …….

E-safety Governor…………Hazel Mallett…………………………………… on   14/ 09/ 2022

Appendix 1

Responding to incidents of misuse – flow chart

Online Safety Incident

Left branch: Unsuitable materials

Unsuitable materials

↓

Report to the person responsible for Online Safety

↓

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

↓

Debrief on online safety incident → **Record details in incident log**

↓

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

↓

Implement changes

↓

Monitor situation

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

Right branch: Illegal materials

Illegal materials or activities found or suspected

↓

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

↓

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

↓

Await Police response

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

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

↓

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

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

Group: ....

Date: ....

Reason for investigation: ....

....

....

....

Details of first reviewing person

Name: ....

Position: ....

Signature: ....

Details of second reviewing person

Name: ....

Position: ....

Signature: ....

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

....

....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

Reporting Log

Reporting Log Group:						
Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

B1 Training Needs Audit Log

Group: ....

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date

Wraxall Primary School
E-safety Incident Log

Details of all e-safety incidents are to be reported to the ICT co-ordinator, who will record the details in the e-safety log.
This incident log will be monitored by the Headteacher, deputy Headteacher, ICT co-ordinator and chair of governors.
For guidance in the event of an incident, please follow the e-safety incident flowchart.
The SWGfL Internet Safety Protocol can be accessed at the link below.
http://www.swgfl.org.uk/Files/Documents/internet_safety_protocol

E-safety incident	Date -	Time -
Name of person who discovered the incident		
Pupils involved		
Staff involved		
Nature of incident (e.g. cyber bullying, inappropriate material, grooming)		
Full details (including where and when the event occurred)		
Does the incident warrant direct police involvement?		
Contact made with		
Recommended action		
Signature	Person completing log	Headteacher
Review comments Date -		