



# Canon Burrows C of E Primary School

## Online Safety Policy

# Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group made up of:

- Headteacher
- Senior Leaders
- Co-ordinators
- Staff – including Teachers and Technical staff

Consultation with the whole school 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:	January 2023
The implementation of this Online Safety policy will be monitored by the:	Senior Leadership Team and Computing Co-Ordinators
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 (which will include anonymous details of online safety incidents) at regular intervals:	Once a year
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	January 2024
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Safeguarding Lead, LA Safeguarding Officer, LADO and/or Police

The school will monitor the impact of the policy using:

- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - students / pupils
  - parents / carers
  - staff

## **Scope of the Policy**

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / 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**

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will

review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Mrs Dawn Enright – Safeguarding Governor.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

## Headteacher and Senior Leaders

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

## The DSL

Details of the school's designated safeguarding lead (DSL) deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with other senior leaders and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the Network manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, Network manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

## Network Manager / Technical staff

Remedian IT Solutions is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority 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

- 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 / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and Senior Leaders for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

## Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher and Online Safety Officer 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 students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

## Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

## 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, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- responding appropriately to any social media messages or posts that could be detrimental to the good reputation of the school and its staff.
- their children's personal devices in the school

## Community Users

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

## Policy Statements

### Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of *pupils* in online safety / digital literacy is therefore an essential part of the school's online safety provision. Children need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of 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 students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (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 activities
- Letters, newsletters, web site
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. [swgfl.org.uk](http://www.swgfl.org.uk)      [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/)  
<http://www.childnet.com/parents-and-carers>

## **Education – The Wider Community**

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

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community

## **Education & Training – Staff / Volunteers**

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements. It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Officer / Headteacher will receive regular updates through attendance at external training 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 / phase meetings / INSET days.
- The Online Safety Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

## **Training – Governors**

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any 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.
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

## Technical – infrastructure / equipment, filtering and monitoring

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

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

There will be regular reviews and audits of the safety and security of school technical systems

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password (KS2 and above) by Remedian IT Solutions 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 at regular intervals.
- The “master / administrator” passwords for the school ICT systems, used by the Network Manager (or other person) must also be available to the *Headteacher* and senior leaders and kept in a secure place.
- The school (with the support of Remedian IT Solutions) 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 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, [report to Online Safety Officer or DSL, request made to Remedian IT to make filtering change](#).
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced / differentiated user-level filtering
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.

- An agreed policy 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.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

## Mobile Technologies (including BYOD/BYOT)

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

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

- The school Acceptable Use Agreements for staff, pupils/students and parents / carers will give consideration to the use of mobile technologies
- The school allows:

	<b>School owned for single user</b>	<b>School owned for multiple users</b>	<b>Student owned</b>	<b>Staff owned</b>	<b>Visitor owned</b>
Allowed in school	Yes	Yes	Yes	Yes	Yes
Full network access	Yes	Yes	No	No	No
Internet only	Yes	Yes	No	Yes <i>(Guest Wi-Fi)</i>	No
No network access			Yes	Yes	Yes

## Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images

may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students / 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 students / 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 is 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.
- School will take all reasonable measures to ensure that photographs of pupils or staff are not published without permission from parents/ carers/ staff.
- 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.
- Photographs of pupils may be taken by event organisers and media. The school is not in control of the publication of these images and parents will need to consider this when granting permission for children to attend events.

## 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 Policy (GDPR Privacy Notice) which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

**Staff must ensure that they:**

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

When personal data is stored on any portable computer system:

- The data must be encrypted and password protected.
- Memory sticks are not to be used.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

## Communications

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

Communication Technologies	Staff & other adults				Pupils		
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Not allowed
Mobile phones may be brought to the school							
Use of mobile phones in lessons							
Use of mobile phones in social time							
Taking photos on mobile phones / cameras							
Use of other mobile devices e.g. tablets, gaming devices							
Use of personal email addresses in school, or on school network							
Use of school email for personal emails							
Use of messaging apps							
Use of social media							
Use of blogs							

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff 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 (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 students / pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils 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 and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority 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 students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

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

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

#### Personal Use:

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

#### 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's use of social media for professional purposes will be checked regularly to ensure compliance with the school's policies.

## Dealing with unsuitable / inappropriate activities

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

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

## User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978				X	
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.				X	
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008				X	
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986				X	
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
	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	

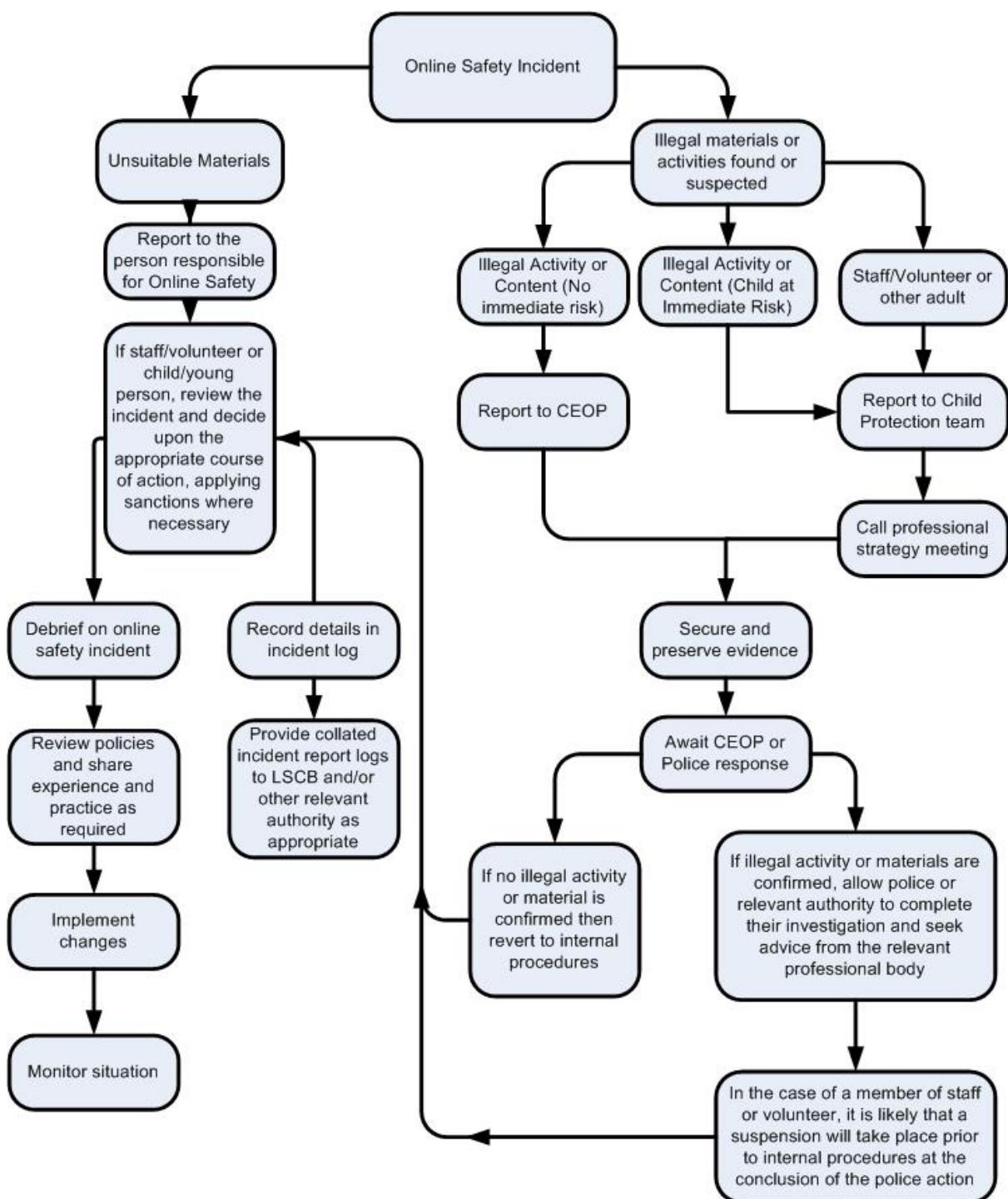
On-line gaming (educational)	X		
On-line gaming (non-educational)		X	
On-line gambling		X	
On-line shopping / commerce	X		
File sharing		X	
Use of social media		X	
Use of messaging apps		X	
Use of video broadcasting e.g. Youtube		X	

## Responding to incidents of misuse

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

### Illegal Incidents

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



## Other Incidents

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

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

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

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

## School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Pupils 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 class teacher	Refer to Safeguarding Lead (or Deputy)	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers
Unauthorised use of non-educational sites during lessons	X	X	X		X	X
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device		X	X		X	X
Unauthorised / inappropriate use of social media / messaging apps / personal email		X	X		X	X
Unauthorised downloading or uploading of files			X		X	X
Allowing others to access school network by sharing username and passwords		X	X		X	X
Attempting to access or accessing the school network, using another student's / pupil's account	X	X		X	X	X
Attempting to access or accessing the school network, using the account of a member of staff	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
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	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X				X	
Deliberately accessing or trying to access offensive or pornographic material		X	X			X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X			X	X	X

#### **Actions / Sanctions**

	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email		X				X		
Unauthorised downloading or uploading of files	X						X	
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X					X	

## Staff Incidents

Careless use of personal data e.g. holding or transferring data in an insecure manner	X			X	
Deliberate actions to breach data protection or network security rules	X		X	X	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X		X	X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X		X	X	
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with students / pupils	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
Using proxy sites or other means to subvert the school's filtering system	X	X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X			X	
Deliberately accessing or trying to access offensive or pornographic material	X	X			X
Breaching copyright or licensing regulations	X	X			X
Continued infringements of the above, following previous warnings or sanctions				X	X

© Adapted from the South West Grid for Learning Trust Ltd 2018

# Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

**Name of pupil:**

**When I use the school's ICT systems (like computers) and get onto the internet in school I will:**

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
  - I click on a website by mistake
  - I receive messages from people I don't know
  - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**

**Signed (pupil):**

**Date:**

**Parent/carer agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

**Signed (parent/carer):**

**Date:**

# Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
<b>Name of pupil:</b>	
<b>I will read and follow the rules in the acceptable use agreement policy.</b>	
<b>When I use the school's ICT systems (like computers) and get onto the internet in school I will:</b>	
<ul style="list-style-type: none"><li>• Always use the school's ICT systems and the internet responsibly and for educational purposes only</li><li>• Only use them when a teacher is present, or with a teacher's permission</li><li>• Keep my usernames and passwords safe and not share these with others</li><li>• Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer</li><li>• Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others</li><li>• Always log off or shut down a computer when I've finished working on it</li></ul>	
<b>I will not:</b>	
<ul style="list-style-type: none"><li>• Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity</li><li>• Open any attachments in emails, or follow any links in emails, without first checking with a teacher</li><li>• Use any inappropriate language when communicating online, including in emails</li><li>• Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate</li><li>• Log in to the school's network using someone else's details</li><li>• Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision</li></ul>	
<b>If I bring a personal mobile phone or other personal electronic device into school:</b>	
<ul style="list-style-type: none"><li>• I will hand my phone into my teacher first thing in the morning and not use my phone again until hometime.</li><li>• I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission</li><li>• I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online</li></ul>	
<b>I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.</b>	
<b>Signed (pupil):</b>	<b>Date:</b>

ACCEPTABLE USE OF THE SCHOOL' S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS  
AND PARENTS/CARERS

**Parent/carer' s agreement:** I agree that my child can use the school' s ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school' s ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

**Signed (parent/carer):**

**Date:**

# Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
<b>Name of staff member/governor/volunteer/visitor:</b>	
<b>When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:</b>	
<ul style="list-style-type: none"><li>• Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)</li><li>• Use them in any way which could harm the school's reputation</li><li>• Access social networking sites or chat rooms</li><li>• Use any improper language when communicating online, including in emails or other messaging services</li><li>• Install any unauthorised software, or connect unauthorised hardware or devices to the school's network</li><li>• Share my password with others or log in to the school's network using someone else's details</li><li>• Take photographs of pupils using my personal device.</li><li>• Share confidential information about the school, its pupils or staff, or other members of the community</li><li>• Access, modify or share data I'm not authorised to access, modify or share</li><li>• Promote private businesses, unless that business is directly related to the school</li></ul>	
<p>I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.</p> <p>I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.</p> <p>I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.</p> <p>I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.</p> <p>I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.</p>	
<b>Signed (staff member/governor/volunteer/visitor):</b>	<b>Date:</b>

## **Appendix 4: Online safety training needs - self audit for staff**

<b>ONLINE SAFETY TRAINING NEEDS AUDIT</b>	
<b>Name of staff member/volunteer:</b>	<b>Date:</b>
<b>Question</b>	<b>Yes/No (add comments if necessary)</b>
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	