WHITGREAVE PRIMARY SCHOOL

E-SAFETY AND ACCEPTABLE USE POLICY

Mrs Butters – Computing and E-safety Lead

Adapted from the SWGFL- https://swgfl.org.uk

Whitgreave Primary School

E-safety and Acceptable Use Policy

Schedule for Development/Monitoring/Review

This Online Safety Policy was approved by the Governing Board on:	
The implementation of this Online Safety Policy will be monitored by the:	*DSL, E-safety Lead and Leadership Team*
Monitoring will take place at regular intervals:	*Daily of filtering/ Once a term/ Monthly for logs*
The Governing Board will receive a report on any online safety incidents that occur within school and how these were dealt with.	*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:	*September each year*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	LA Safeguarding Officer LADO Police MASH

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of Internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of
    - pupils
    - parents/carers
    - staff

1. Aims

Our school aims to:

- have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism;
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes;
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation
- The policy also refers to the DfE's guidance on protecting children from radicalisation.
- Furthermore, it reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.
- The policy also takes into account the National Curriculum Computing programmes of study.

3. Roles and Responsibilities

The Governing Board

- The Governing Board has overall responsibility for monitoring this policy and holding the Head Teacher to account for its implementation.
- The Governing Board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL) and E-safety Lead.
- The governor who oversees safeguarding and online safety is Jayne Pownall.

All governors will:

- ensure that 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 (appendix 1-5).
- ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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.

- receive regular training on safeguarding, including online safety.

The Head teacher

- The Head Teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead (DSL)

- Details of the school's DSL and deputies are set out in our Safeguarding Policy as well as relevant Job Descriptions.

The DSL takes lead responsibility for online safety in school alongside our Online Safety Lead by:

- supporting the Head Teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- working with the Head Teacher, Online Safety Lead and ICT 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 Safeguarding Policy.
- ensuring that any online safety incidents are logged on CPOMS (in line with the school Safeguarding Policy) 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.
- liaising with other agencies and/or external services if necessary.
- providing regular reports on online safety in school to the Head Teacher and/or Governing Board.

This list is not intended to be exhaustive.

The E-Safety/Computing Lead

The E-Safety/ Computing Lead will:

- ensure that any online safety incidents are logged on CPOMS (in line with the school Safeguarding Policy) and dealt with appropriately in line with this policy.
- ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Behaviour Policy.
- update and deliver staff training on online safety.
- liaise with other agencies and/or external services if necessary.
- provide regular reports on online safety in school to the Head Teacher and/or Governing Board.
- complete an annual e-safety risk assessment that considers and reflects the risks our children face.
- complete monthly checks on the filtering and monitoring systems (log completed).

This list is not intended to be exhaustive.

The ICT manager (Spark IT)

The ICT manager, in conjunction with the Online Safety Lead is responsible for:

- putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- conducting a full security check and monitoring the school's ICT systems on a regular basis.
- blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- ensuring that any technical online safety incidents are logged (see appendix 8) and dealt with appropriately in line with this policy.

This list is not intended to be exhaustive.

All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- maintaining an understanding of this policy.
- implementing this policy consistently.
- agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 4), and ensuring that pupils follow the school's terms on acceptable use.
- working with the DSL to ensure that any online safety incidents are logged on CPOMS (in line with the school Safeguarding Policy) and dealt with appropriately in line with this policy.
- ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour Policy.
- responding appropriately to all reports and concerns about sexual violence and/or harassment, child on child abuse (including cyberbullying) both online and offline and maintaining an attitude of 'it could happen here'.
- have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices.
- have read, understood and signed the Staff Acceptable Use Policy (AUP).
- report any suspected misuse or problem to the Head Teacher/DSL/Senior Leader/Online Safety Lead for investigation/action/sanction.
- ensure all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems.
- ensure online safety issues are embedded in all aspects of the curriculum and other activities.
- ensure pupils understand and follow the Online Safety Policy and Acceptable Use policies.
- ensure pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- monitor the use of digital technologies, mobile devices (tablets), cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.

- In lessons where the Internet is used, this should be pre-planned and 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.

This list is not intended to be exhaustive.

Pupils

Pupils are expected to:

- be 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.
- understand the importance of reporting abuse (including child on child), misuse or access to inappropriate materials and know how to do so.
- 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

Parents are expected to:

- Notify a member of staff or the Head Teacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2).
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

Parents and carers will be encouraged to support the *school* in promoting good online safety practice and to follow guidelines on the appropriate us:

- digital and video images taken at school events
- access to parents' sections of the website
- Facebook page

Visitors and Members of the Community

- Visitors and members of the community who use the school's ICT systems or Internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 5).

4. Educating Pupils about Online Safety

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

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

- A planned online safety curriculum should be provided as part of Computing/PD/other lessons and should be regularly revisited (The school currently uses Rising Stars Scheme of Work).
- Key online safety messages should be reinforced as part of a planned assemblies and morning work.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the 'Pupil Acceptable Use Agreement' and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the Internet and mobile devices.
- In lessons where Internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches (appendix 8).
- Where pupils are allowed to freely search the Internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in Internet searches being blocked. In such a situation, staff can request that the Technical Staff 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 (see appendix 9).

National Curriculum

All schools have to teach:

Relationships education and health education in primary schools

In **Key Stage 1**, pupils will be taught to:

- use technology safely and respectfully, keeping personal information private.

- identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

In **Key Stage 2**, pupils will be taught to:

- use technology safely, respectfully and responsibly.
- recognise acceptable and unacceptable behaviour.
- identify a range of ways to report concerns about content and contact.

By the **end of primary school**, pupils will know:

- that people sometimes behave differently online, including by pretending to be someone they are not.
- that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- how information and data is shared and used online.
- what sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
- how to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

The safe use of social media and the Internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating Parents about Online Safety

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/meetings
- letters, newsletters, web site, Facebook page
- parents/carers evenings sessions
- Safeguarding Newsletter (including information about cyberbullying)
- high profile events/campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers
- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Class Teacher, Phase Leader, Online Safety Lead or the DSL.

- Concerns or queries about this policy can be raised with any member of staff or the Head Teacher.

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.
- sharing their online safety expertise/good practice with other local schools.

6. Training

- All new staff members will receive training, as part of their induction, on safe Internet use and online safeguarding issues including cyberbullying, child on child abuse, consensual and non-consensual sharing of images, the risks of online radicalisation and reporting on CPOMS.
- All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
    - abusive, harassing, and misogynistic messages
    - non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - sharing of abusive images and pornography, to those who don't want to receive such content
    - cyberbullying
    - upskirting
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse.
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up.
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable

More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

7. Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Behaviour Policy and Anti-Bullying Policy.)

Preventing and Addressing Cyberbullying

- To help prevent cyberbullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
- The school will actively discuss cyberbullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyberbullying with their classes.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes Personal Development (PD) education, and other subjects where appropriate.
- All staff, governors and volunteers (where appropriate) receive training on cyberbullying, its impact and ways to support pupils, as part of safeguarding training.
- The school also sends information/leaflets on cyberbullying to parents (within the Safeguarding Newsletter) so that they are aware of the signs, how to report it and how they can support children who may be affected.
- In relation to a specific incident of cyberbullying, the school will follow the processes set out in the School Behaviour and Anti-Bullying Policies. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
- The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining Electronic Devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Technical – Infrastructure/Equipment, Filtering and Monitoring

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

- The school's 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.
- Our 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.
- Where appropriate, users will be provided with a username and secure password by the school technician (SPARK IT). Users are responsible for the security of their username and password.
- The "master/administrator" passwords for the school systems, used by the Network Manager (or other person) must also be available to the Head Teacher or other nominated Senior Leader and kept in a secure place (e.g. school safe).
- SPARK IT and the Computing leads are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- All requests for filtering changes should go to the Computing/E-safety Lead.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the Internet.
- The school has enhanced/differentiated user-level filtering.
- School technical staff/ E-safety Lead will monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

8. Acceptable Use of the Internet in School

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the Internet (appendices 1-5). Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.

Use of the school's Internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1-5.

9. Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop, SMART watches 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 other cloud based services such as email and data storage.

The use of mobile phones and devices such as SMART watches within lessons, corridors and classrooms (during the school day) is not permitted. This includes making and receiving calls, recording videos or audio, taking photos and sharing images. Pupils are not permitted to wear SMART watches in lessons and should be handed into the School Office or class teacher at the beginning of the day if worn to school.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Staff Code of Conduct, Behaviour 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:

	School Devices	Personal Devices

	School owned for single user	School owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*In certain circumstances*	*No*
Internet Only					*Yes*	*Yes*
No network access				*Yes*		*Yes*

Use of Digital and Video Images

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

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the Internet e.g. on social networking sites.
- All digital images taken, must be taken on a school device and not personal equipment.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/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 (phones, cameras or SMART watches) 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.

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. (See schools data protection policies for further information)

When personal data is stored on any mobile device or removable media the:

- Data must be encrypted and password protected.
- Device must be password protected.
- Device must be protected by up to date virus and malware checking software.
- Data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

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.
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- Can help data subjects understand their rights and know how to handle a request whether verbal or written.
- Where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- Staff will not transfer any school personal data to personal devices except as in line with school policy.
- Access personal data sources and records 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.

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				Students/Pupils			
	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	x					x		
Use of mobile phones in lessons				x				x
Use of mobile phones in social time		x						x
Taking photos/videos/audio recordings on mobile phones				x				x
Taking photos/videos/audio recordings on SMART watches (personal)				x				x
Taking photos on cameras (personal)				x				x
Taking photos on cameras/ tablets (school)	x					x		
Use of other mobile devices e.g. smart watches, tablets, gaming devices		x						x
Use of personal email addresses in school, or on school network		x						x
Use of school email for personal emails		x						x
Use of messaging apps		x						x
Use of social media		x						x
Use of blogs		x				x		

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, school texts 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.
- All children bringing mobile phones into school must hand them into the Class Teacher/School Office at the beginning of the day and collect them at the end of the day.

10. Social Media - Protecting Professional Identity

All schools 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 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.

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.

See Social Media policy for more details.

11. How the school will Respond to Issues of Misuse

Where a pupil misuses the school's ICT systems or Internet, we will follow the procedures set out in our policies on behaviour. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the Internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

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:

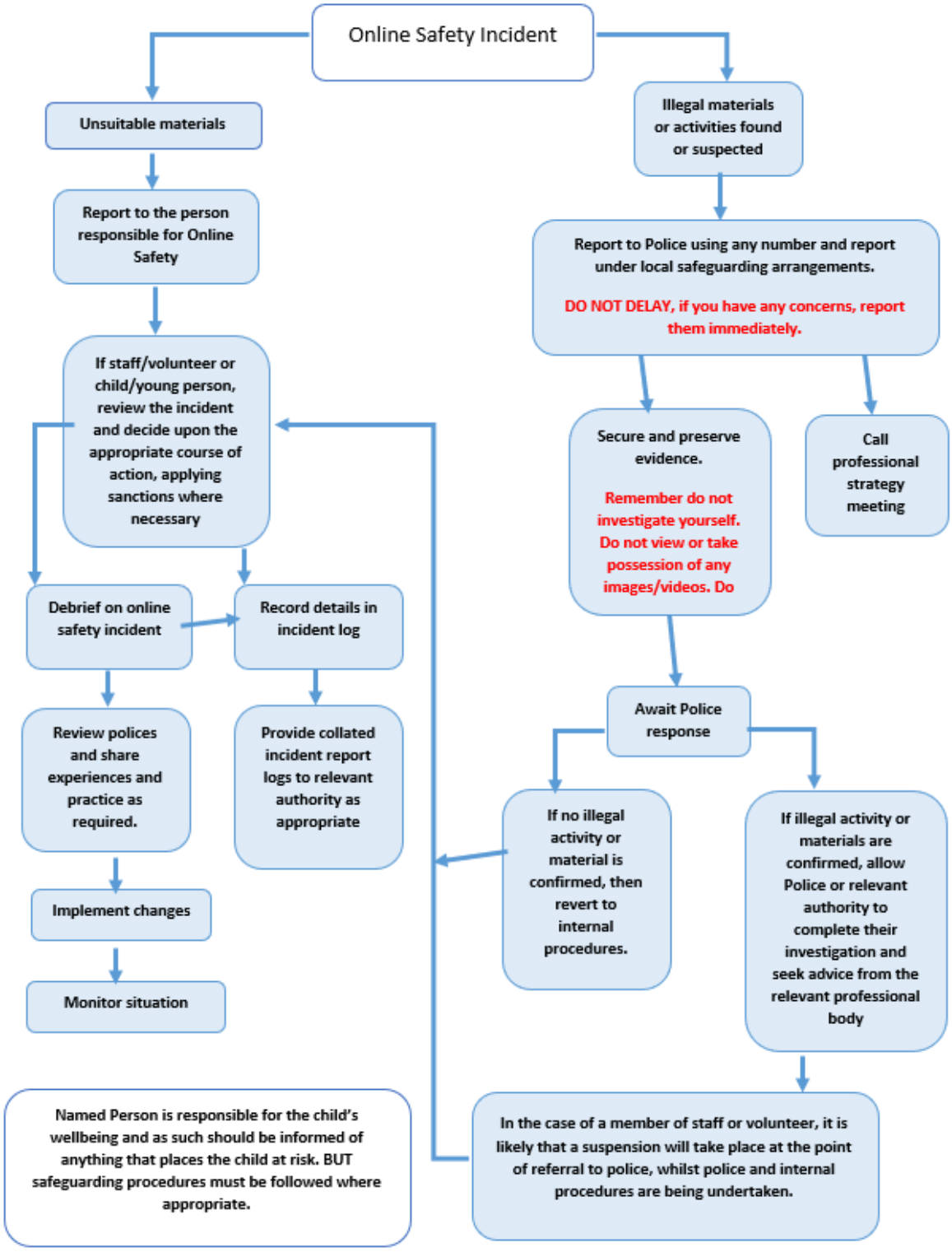
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicat	Child sexual abuse images –The making, production or distribution of indecent images 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

e or pass on, material, remarks, proposals or comments that contain or relate to:	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					X	
Using school systems to run a private business					X	
Infringing copyright					X	
On-line gaming (educational)	X					
On-line gaming (non-educational)					X	
On-line gambling					X	
On-line shopping/commerce		x				
File sharing		x				

Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting e.g. Youtube (viewing)	x				
Use of video broadcasting e.g. Youtube (uploading)		x			

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 6) 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:

- The school will 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
    - 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 (see appendix 7) should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

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

Students/Pupils Incidents	Actions/Sanctions								
	Refer to Class Teacher	Refer to Phase Leader	Refer to Headteacher	Refer to Police	Refer to Technical Support Staff for action re filtering/security etc.	Inform Parents/Carers	Removal of network/internet access rights	Warning	Further sanction e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X		X	x	x	x
Unauthorised use of non-educational sites during lessons	x	x	X			X	x	x	X
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	x	x	X			X	x	x	X
Unauthorised/inappropriate use of social media/ messaging apps/personal email	x	x	X			X	x	x	X
Unauthorised downloading or uploading of files	x	x	X			X	x	x	X
Allowing others to access school network by sharing username and passwords	x	X	x			X	x	x	X
Attempting to access or accessing the school network, using another student's/pupil's account	x	x	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	x	X
Corrupting or destroying the data of other users		x	X			X	x	x	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			x			X	x	x	X
Continued infringements of the above, following previous warnings or sanctions			X			X			X
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	x

Accidentally accessing offensive or pornographic material and failing to report the incident	x				x	X			
Deliberately accessing or trying to access offensive or pornographic material			x		x	X	x	x	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	x	x	x		x	X	x	x	X

Actions/Sanctions

Staff Incidents	Refer to Line Manager	Refer to Headteacher	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X			x	X
Inappropriate personal use of the internet/social media/personal email	x	x	X			x	x	X
Unauthorised downloading or uploading of files	x	X			x	x	x	X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	x	X				X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	x	x	X			x	x	X
Deliberate actions to breach data protection or network security rules	x	x	X			x	x	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x	x	X			x	x	x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x	X	x			x	X

Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils	x	X	X	x		x	x	X
Actions which could compromise the staff member's professional standing	x	x	X			x	x	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x	x	X			x	x	X
Using proxy sites or other means to subvert the school's filtering system	x	x	X			x	X	x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	X			x	x	
Deliberately accessing or trying to access offensive or pornographic material		x	X	X				
Breaching copyright or licensing regulations	x					X		
Continued infringements of the above, following previous warnings or sanctions	x	x	X				x	X

12. Monitoring Arrangements

The DSL and E-safety Lead actions and monitors E-safety and safeguarding issues related to online safety on CPOMS in line with the Safeguarding Policy. The DSL/E-safety Lead will monitor current trends and identify areas that pupils/staff/parents may need additional support with.

This policy will be reviewed every year. At every review, the policy will be shared with the Governing Board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Remote Teaching

In the eventuality of needing to teach remotely, all online teaching should follow the same principles as set out in the E-Safety and Acceptable Use Policy.

- We will ensure any use of online learning tools and systems are in line with privacy and data protection/GDPR requirements.
- All procedures and expectations stated in the main E-Safety Policy must continue to be adhered to.
- Parents will be reminded of the support available to them in order to help to keep their children safe online through the website, Safer Internet day, leaflets and the School Facebook page.
- Wherever possible, staff should use school equipment for setting online learning and communications with parents/carers and children.

Home Learning

- The majority of home learning will be set using the learning platforms provided by the school- Google Classrooms and Tapestry.
- All children have a 'work pack' which will be sent/delivered to their home and used in support of the online learning.
- These are secure authenticated platforms for which children have unique logins.
- Where children are directed to alternative websites, for example to access video resources, staff will check the suitability of the content before directing children to access them.
- Staff will wear suitable clothing, as should anyone else in their household if recording or videoing, e.g. a story time session for children.
- Staff will be mindful of what can be seen and heard in the background if making a video or voice recording.
- Language must be professional and appropriate at all times, including any family members in the background.
- Staff must only use platforms provided by the school (Google classrooms and Tapestry) to communicate with pupils.
- When children are invited to a class zoom/classroom meeting (assembly, book reading), these will be recorded to safeguard the children and members of staff in these virtual meetings. The recordings will be held in accordance of the GDPR regulations.
- Staff should NOT use 'live' conferencing to communicate with parents/carers or pupils unless it is in the allocated assembly times.
- Children are able to communicate via private messages and email with teachers through Google Classroom and Tapestry. This is an enclosed email system – children are unable to send emails outside of school members.
- Children in Year 1-6 are communicate with each other on the live streams and this is monitored by the Class Teacher who is able to remove and mute pupil's comments if inappropriate.
- Where possible calls to children will be made from school telephones. When this is not feasible and staff are calling children from their own telephones, they will always use 141 before dialling so as not to share their personal telephone numbers.

Reporting Procedures

- An essential part of the online planning process will be ensuring children who are being asked to work online have very clear reporting routes in place so they can raise any concerns whilst online. Children are able to report inappropriate comments to their teacher via private messages and streams.
- Parents/carers being directed to sites that support them in raising concerns e.g. Thinkuknow.
- Parents emailing or calling the school office to inform staff of concerns
- Staff are to follow normal safeguarding procedures and follow safeguarding addendum to report missing children or any comments raising online.

Appendix 1

Pupil Acceptable Use Agreement – KS2

School policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This Acceptable Use Agreement is intended to ensure:

- Young people will be responsible users and stay safe while using the Internet and other digital technologies for educational, personal and recreational use.
- The school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users.

Acceptable Use Agreement

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

For my own personal safety:

- I understand that the *school* will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.).
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I will be respectful and work hard if I need to complete remote learning.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the *school* systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the *school* systems or devices for on-line gaming, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the *school*:

- I will only use my own personal devices (USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the *school*, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not use social media sites on school equipment.

When using the Internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the *school* also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, loss of playtimes/lunchtimes/golden times, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Pupil Acceptable Use Agreement Form

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

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the *school* systems and devices (both in and out of school)
- I use my own equipment out of the school in a way that is related to me being a member of this *school* e.g. communicating with other members of the school, website etc.

Name of Student/Pupil: .....

Group/Class: .....

Signed: .....

Date: .....

Appendix 2

Pupil Acceptable Use Policy Agreement – EYFS/KS1

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of computers/tablets and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer/tablet.
- I will be respectful and work hard if I need to complete remote learning.

KS1 Signed (child): .....

EYFS Signed (parent): .....

Appendix 3

Parent/Carer Acceptable Use Agreement

Dear Parents/Carers,

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect all pupils to agree to be responsible users. Please read and sign the Acceptable Use Agreement to allow your child access to our Internet and ICT systems at school and to show your support of the school in this important aspect of the school's work.

As the parent/carer, I give permission for my son/daughter to have access to the Internet and to ICT systems at school.

- I understand that the school will discuss the Acceptable Use Agreement with my son/daughter and they will understand that they will need to follow the school rules.

- I understand that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the Internet – both in and out of school - and that this will be regularly revisited during e-safety lessons.

- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the Internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the Internet and using mobile technologies.

- I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

- I will encourage my child to adopt safe use of the Internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Name of Parent/Carer:_____

Child's Name:_____

Signature of Parent/Carer: _____Date:_____

Appendix 4

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

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

This Acceptable Use Policy is intended to ensure:

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

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

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the *school/* will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- During remote learning, if participating any live teaching e.g. assemblies, book time, I will only use platforms provided by the school and ensure that these are recorded to safeguard myself and the children.
- During remote learning, I will ensure that the resources the children are being directed to are appropriate and suitable for them.
- I will report any concerns I have regarding online safety and safeguarding (including child on child abuse) to the appropriate person through CPOMS in a timely manner so that this can be actioned.

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

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

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

- When I use my mobile devices (including SMART watches) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses for school business or communications on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless permission is granted.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

- I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the

premises and my use of personal equipment on the premises or in situations related to my employment by the school.

- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

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

Staff/Volunteer Name: .....

Signed: .....

Date: .....

Appendix 5

Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

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

Acceptable Use Agreement

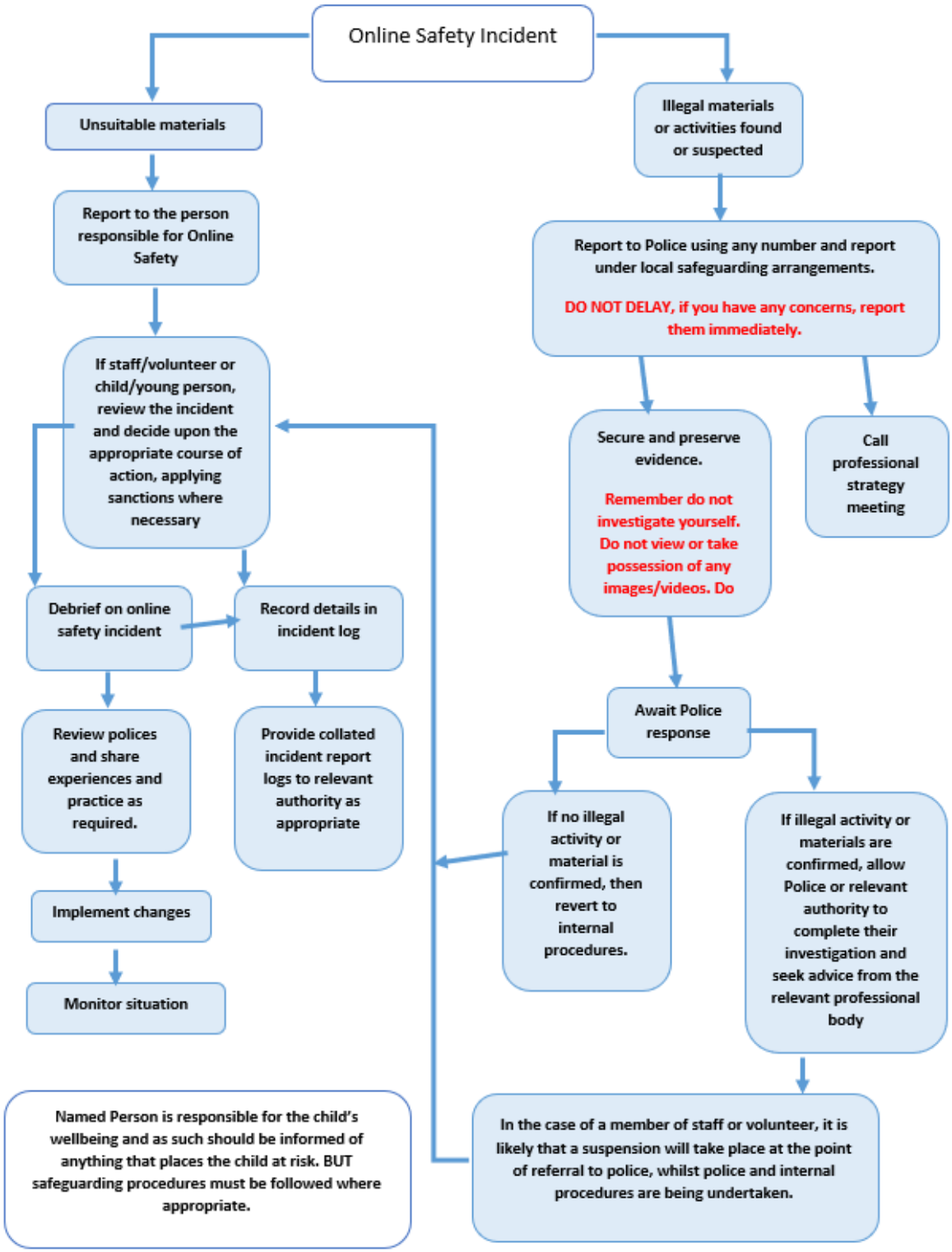
I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

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

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

Appendix 6 ..... Signed: ..... Date:.....

Responding to incidents of misuse – flow chart



Appendix 7

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

Appendix 8

Internet Filtering and Monitoring- Reporting an incident

Date:	
Lesson/Classroom:	
Device used:	
What was found- Website/Image found:	
Please explain circumstances of image/website being found e.g. google search, website search etc. Please be as specific as possible.	
Person reporting incident:	
Action taken by DSL/E-safety Lead/Computing Lead:	

Appendix 9

Internet Filtering and Monitoring- Requesting filtering to be removed

Date:	
Lesson/Classroom/teacher:	
Device to be used:	
What website/ key words need to be unblocked?	
Please explain why this is needed e.g curriculum area/lesson etc	
Temporary or permanent? If temporary please give a date when it can be blocked again	
Person reporting incident:	
Action taken by DSL/E-safety Lead/Computing Lead:	

Appendix 10: Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/

South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/

Childnet – http://www.childnet-int.org/

Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline

Revenge Porn Helpline - https://revengepornhelpline.org.uk/

Internet Watch Foundation - https://www.iwf.org.uk/

Report Harmful Content - https://reportharmfulcontent.com/

CEOP

CEOP - http://ceop.police.uk/

ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources

Kent – Online Safety Resources page

INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/

UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Netsmartz - http://www.netsmartz.org/

Tools for Schools

Online Safety BOOST – https://boost.swgfl.org.uk/

360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

360Data – online data protection self-review tool: www.360data.org.uk

SWGfL Test filtering - http://testfiltering.com/

UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/

SELMA – Hacking Hate - https://selma.swgfl.co.uk

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/

Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388

DfE - Cyberbullying guidance -
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – Cyberbullying guidance and practical PSHE toolkit:
http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harrassment
UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking
UKSIC - Safety Features on Social Networks
Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Evolve - https://projectevolve.co.uk
UKCCIS – Education for a connected world framework
Teach Today – www.teachtoday.eu/
Insafe - Education Resources

Data Protection

360data - free questionnaire and data protection self review tool
ICO Guides for Education (wide range of sector specific guides)
DfE advice on Cloud software services and the Data Protection Act
IRMS - Records Management Toolkit for Schools
NHS - Caldicott Principles (information that must be released)
ICO Guidance on taking photos in schools
Dotkumo - Best practice guide to using photos

Professional Standards/Staff Training

DfE – Keeping Children Safe in Education
DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet – School Pack for Online Safety Awareness
UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support

UKSIC – Appropriate Filtering and Monitoring
SWGfL Safety & Security Resources
Somerset - Questions for Technical Support
NCA – Guide to the Computer Misuse Act

NEN – Advice and Guidance Notes

Working with parents and carers

Online Safety BOOST Presentations - parent's presentation

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

Get Safe Online - resources for parents

Teach Today - resources for parents workshops/education

Internet Matters

Prevent

Prevent Duty Guidance

Prevent for schools – teaching resources

NCA – Cyber Prevent

Childnet – Trust Me

Research

Ofcom –Media Literacy Research

Further links can be found at the end of the UKCIS Education for a Connected World Framework

Appendix 11: Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MAT	Multi Academy Trust
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
UKCIS	UK Council for Internet Safety
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS Education for a Connected World Framework