Shefford Lower School

Online Safety Policy

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

- Headteacher and Senior Leadership Team
- Staff - including Teachers, Support Staff, Technical staff
- Governors
- Parents and Carers

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

It applies to all members of the school (including staff, children, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems both in and out of the school.

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. Governors will be informed about online safety incidents within termly Headteacher reports. The role of Online Safety Governor is part of the role of the Safeguarding Governor on the Governing Body.

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 Leader (DW, working alongside PR in her role as Designated Safeguarding Deputy.)
- The Headteacher and Deputy Head are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Online Safety Incident flow chart (attached) details to procedure that any staff facing an issue, disclosure or report, need to follow.
- Online Safety Incidents or concerns should also be reported on CPOMs as appropriate, in accordance with safeguarding procedures.
- The Headteacher is responsible for ensuring that the Online Safety Leader receives suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Leader.

Online Safety Leader:

- leads the Online Safety Group.
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff.
- liaises with the Local Authority / relevant body.
- liaises with school technical staff.
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- reports regularly to the Headteacher.

Network Managers and Technical staff:

The Network Managers (DWM), Technical Staff (DWM and Learning Resources Co-ordinator) and the Computing/Online Safety Leader (DW) are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack: firewall and anti-virus protection is in place and these and system updates are performed as necessary.
- that the school meets required online safety technical requirements and any Local Authority Online Safety Policy 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.
- Filtering, which is appropriate and in accordance with the DfE's Keeping Children Safe in Education guidance, is applied and updated on a regular basis.
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- that the use of the network / internet / Learning Platform / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction.
- that monitoring software / systems are implemented and updated as agreed in school policies.
- The 360 safe self-review framework tool is being used. The Revised Prevent Duty Guidance: for England and Wales 2015 requires that we "assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology".

Teaching and Support Staff:

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices.

- they have read, understood and signed the Staff Acceptable Use Policy (AUP).
- they report any suspected misuse or problem to the Headteacher for investigation / action / sanction.
- all digital communications with children / 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.
- children understand and follow the Online Safety Policy and acceptable use policies.
- children 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, children 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
- cyber-bullying

Online Safety Group:

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives.

Members of the Online Safety Group will assist the Online Safety Leader with:

- the production / review / monitoring of the school Online Safety Policy / documents.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet.
- consulting stakeholders – including parents / carers and the children about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool.

Children:

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

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Learning Platform 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 will be asked to agree to and follow guidelines on the appropriate use of:

- digital and video images taken at school events.
- access to parents' sections of the website / Learning Platform
- Social media use outside of school. Parents are asked not to post names of other children at the school online or photos of staff. They are also reminded that they or their children must not to ask to "friend" staff members. As a school we expect that children adhere to the legal age limitations on social media use outside of school and do not have their own accounts set up, and parents are made aware that we would seek to have children's profiles removed, should any be discovered.

Community Users/Visitors

Community Users who access school systems will be expected to sign a Community User Acceptable Use Agreement before being provided with access to school systems. They will be logged in as guests (with no access to school network folders) and would be monitored during their use of our equipment/internet.

Policy Statements

Education – children :

Whilst regulation and technical solutions are very important, their use must be balanced by educating children to take a responsible approach. The education of children in online safety 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 is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities. It will be provided in the following ways:

- A planned online safety curriculum is provided as part of Computing and Life Learning lessons. It is explicitly taught in some Computing and Life Learning lessons and other opportunities are taken to reinforce or consolidate the children's understanding of Online Safety are planned into other lessons or units of work as appropriate.
- Key online safety messages are reinforced as part of a planned teaching programme, which included activities planned to highlight awareness on Internet Safety Day.
- Children 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.
- Children are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Children are 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.
- Children are 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 act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, children are guided to sites checked as suitable for their use, where possible or appropriate. It is recognised that when children are developing online searching skills, this may not be the case. Children are taught what to do in the event of unsuitable material being found in internet searches both in and out of school and that processes are in place for dealing with this.
- Where children are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit and report sites that need to be blocked by the school's filtering system.

Education – Parents / Carers :

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, the school web site, the Learning Platform, Digital Parenting magazine

- Parents / Carers information evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to relevant web sites / publications
  e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community:

From time to time, the school may 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:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online Safety provision.

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:

- Online safety training will take place annually. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. We arrange a Bedfordshire Police Online Safety training session for staff, and parent sessions (that all staff are invited to), on alternate years. Staff who do not attend the parent sessions will be provided with relevant updates.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Leader or Learning Resources Co-ordinator will provide advice / guidance / training to individuals as required.

Training – Governors :

Governors are invited to attend online safety training / awareness sessions, with particular importance for those who are members of any group involved in online safety.

Technical – infrastructure / equipment, filtering and monitoring :

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

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling are securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users at KS2 will be provided with a username and will create their own secure password, when learning about this aspect of online safety at the start of Year 3 and 4. The Learning Resources Co-ordinator will keep an up to date record of pupil usernames and passwords on the drive only authorised to be accessed by Office users. Users are taught to be responsible for the security of their username and password and will be required to change their password every academic year.
- An administrator password for the school ICT system, is available to the Headteacher, Deputy, Business Manager, Computing Leader and Learning Resources Co-ordinator.
- DWM is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list.
- Internet filtering ensures that children are safe from terrorist and extremist material when accessing the internet.
- The school has differentiated user-level filtering (allowing different filtering levels for different ages / key stages and different groups of users – staff, children)
- School technical staff are able to 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 Online Safety Leader.
- 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 procedure is in place that staff may only take school devices out of school after signing an agreement held by the Business Manager, and only to undertake work related activities.
- Staff users do not have permissions to allow downloading of executable files and installing programmes on school devices, they must contact system administrator to do this.
- An agreed procedure is in place that allows staff to open zipped files containing work related materials when these are received from another member of staff, or are from a trusted website.

- An agreed procedure is in place allowing the use of removable media for non-sensitive data (eg memory sticks / CDs / DVDs) by users on school devices. Personal data is not allowed to be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies :

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, smartwatch, tablet, notebook/laptop or other technology that has the capability of utilising the school's wireless network and the wider internet.

All users should understand that the primary purpose of the use of mobile devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety curriculum.

- The school Acceptable Use Agreements for staff and children will give consideration to the use of mobile technologies

School devices:

- Children are not allowed to bring electronic devices with connectivity or cameras (e.g. phones, tablets, watches) into school.
- Each of the main classes are allocated an iPad and a laptop for professional use in school. These have a staff level of access to the internet and school network and are not to be used by children unsupervised.
- There are 30 iPads and 37 laptops for use by the children. There are 16 additional tablets dedicated to use in the EYFS. The tablet devices all have a children's level of filtered access to the internet; the laptops require log in details which then allocate the relevant level of filtered access to the internet and school network.
- Management of devices / installation of apps / changing of settings / monitoring are undertaken by DWM and the Learning Resources Co-ordinator.
- The school has a right to take, examine and search users' devices in the case of misuse (England only) – n.b. this must also be included in the Behaviour Policy.

Use of digital and video images :

- When using digital images, staff will inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, children 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 children 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. To respect everyone's privacy and in some cases protection, parents are told that these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other children 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 are only taken on school equipment; the personal equipment of staff will not be used for such purposes.
- Care should be taken when taking digital / video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Children must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.
- Children' 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:

Over the course of the next few months, the new GDPR legislation will come into force and the scope and impact of this will be fully detailed in a GDPR Policy.

Presently, the Data Protection Act 1998, details how personal data will be recorded, processed, transferred and made available. This states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- 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.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". It has a Data Protection Policy.
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

Staff must ensure that they:

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

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

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications:

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 can be 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, 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 parents / carers 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.
- Children 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:

School staff should ensure that:

- No reference should be made in social media to children, 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.
- 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.
- 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.

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 and consider the impact to the school's image and reputation.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

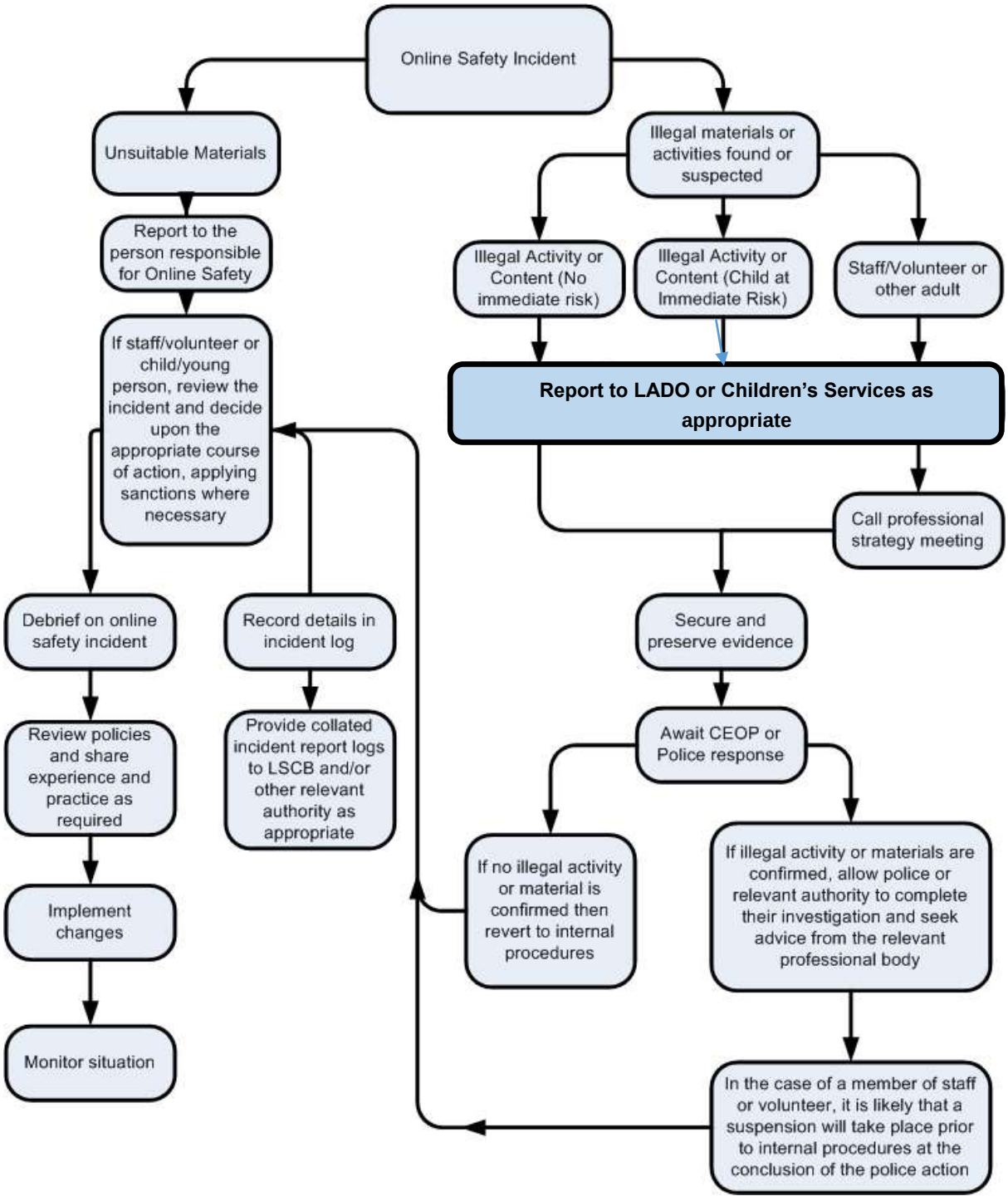
Unsuitable / inappropriate activities:

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.

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) 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, the Headteacher will seek advice from the LADO, Children's Services, and/or the Local Authority as appropriate.

- If content being reviewed includes images of Child abuse then the case will be 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
- The computer in question will be isolated where possible: 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.

Date reviewed	January 2018
Next review date	January 2020
Headteacher **Other Lead staff**	Tracey Callender Polly Ross, Duncan Wakefield, Amanda Burrett
Safeguarding Governor	Jenni Wood,
Chair of Governors	Val Thompson

Appendix 1

Acceptable Use policy

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 children 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 children 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 and record 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. email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are intended for educational use only.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I understand that mobile phones are only permitted in agreed areas, away from the children.
- I also understand that I am not permitted to wear a smartwatch with internet or mobile connectivity at school, or use any personal device capable or taking children's photographs.

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

- 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. Where these images are published on the school website it will not be possible to identify by name, or other personal information, those who are featured.
- Only office staff will use social networking sites in school, in accordance with the school's policies and only for the purposes of monitoring the school's reputation or keeping parents up to date.
- I will only communicate with children 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 (laptops / tablets / mobile phones / USB devices etc) 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 on the school ICT systems.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based protected and restricted data must be held in lockable storage.

- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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 Policy 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 2

Acceptable Use Policy Children

This Acceptable Use Policy is intended to ensure:

- that children will be responsible users and know how to 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.

The school will ensure that all children will have good access to digital technology to enhance their learning opportunities and will, in return, expect children to agree to be responsible users. The school has adapted the children' acceptable use agreements after discussion with children and to ensure that they are age-appropriate.

Acceptable Use Policy Agreement – Early Years and Year 1

- I will keep my VLE password secret.
- If I see something I don't like, I will tell a grown up.
- I will not tell anyone my name or where I live when using a computer, or send pictures of myself.
- I know that my parents or carers will be told if I break these rules

Acceptable Use Policy Agreement – Year 2

- I will only use my own VLE account and never tell anybody my password.
- When using the Internet, I will never try to look at something I know I shouldn't or send unpleasant messages
- I will never tell anybody online my name or where I live, or send pictures of myself.
- I will never tell anybody online who my friends are or where they live.
- I will tell my teacher if I see anything I should not see and I know that my teacher can read all the messages I send.
- I won't copy work from the Internet and say it is mine.
- I know that my parents or carers will be told if I break these rules

Acceptable Use Policy Agreement – Years 3 and 4

- I will only use my own VLE username and password.
- I will not tell my friends my passwords.
- I will not send unkind messages to people.
- It is up to me to be sensible when using a computer or an iPad
- I won't tell anyone online who I am or where I live.
- I won't put any photos of myself online or send them in an email.

- I won't tell anyone online who my friends are.
- I will never look at anything unpleasant or rude online
- I will tell my teacher if I see anything unpleasant or rude on a computer or iPad.
- I will not copy any material from the Internet and say it is my work.
- I know that my parents or carers will be told if I break these rules.

I have read and understand the above and agree to use the school's technology within these guidelines.

Pupil's Name: .....

Signed: .....

Date: .....