POLICY STATEMENT

eSafety

DRAFTED WITH STAKEHOLDERS	**February 2021**
APPROVED BY GOVERNORS	**February 2021**
TO BE REVIEWED BY	**February 2023**

LONGMEADOW PRIMARY SCHOOL & NURSERY

eSAFETY

Contents

Introduction

New technologies are an essential part of teaching and learning at Longmeadow. Through the teaching of computing and a cross curricular approach technology is becoming embedded within the classrooms at our school. We recognise the important role that technology plays in the everyday lives of children, young people and adults. We take seriously our role to build digitally literate children to prepare them fully for the future. Included within this the school community recognises its role in safeguarding children when using technology and installing in them the skills to use technology safely when using this independently. Our aim is to enable children to have the skills to use technology to build young people with the necessary skills to access life-long learning and employment in a safe and productive way, thus creating the digitally literate citizens of the future.

New technologies and computing encompass a wide range of resources including web based resources, programming and mobile learning. The new technologies the pupils have access to include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms
- Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Apps
- Remote controlled devices
- Gaming including places to chat, send/receive messages and set profiles
- Sound recording devices

At Longmeadow we recognise the constant and fast moving pace of technology in the current climate particularly surrounding the evolution of technology in our society.

Longmeadow views new technologies as exciting and beneficial to children, young people and adults both in and out of education. However, we accept that children's use of new technologies, particularly web based resources are not always adequately monitored. We recognise our responsibility to educate all users on their awareness of the range of risk associated with eSafety. This also means working in partnership with parents and carers to ensure that all parties are educated to ensure children's safety.

Longmeadow eSafety Vision:

At Longmeadow we believe that everyone has the right to be safe when online and using New Technologies. We offer children lots of opportunities to use new technologies and access the online world and educate them to manage risk. As pupils we agree to listen to our teachers when learning about eSafety, use our own log in when using New Technologies and report a problem when something goes wrong.

Roles and Responsibilities

Development of the Policy

This e-safety policy has been developed by the eSafety Leader with a working group made up of*:*

- SLT
- eSafety Coordinator
- Staff – including Teachers, Support Staff, Technical staff
- Governors

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

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Board of Directors / Governing Body / Governors Sub Committee on:	February 2021
The implementation of this e-safety policy will be monitored by the:	eSafety Leader and SLT
Monitoring will take place at regular intervals:	Termly by the eSafety Leader and SLT
The Governing Body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Within the heads report
The eSafety 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 e-safety or incidents that have taken place. The next anticipated review date will be:	February 2022
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	HfL eSafety advisor 01438 844893 Consultation Hub – In liaison with DSL Safeguarding referral – in liaison with DSL Police – In liaison with DSL LADO – In liaison with the DSL

The school will monitor the impact of the policy using:

- Logs of reported incidents though CPOMs monitored by the eSafety Leader
- Monitoring logs of internet activity (including sites visited)
- Pupil interviews
- Staff opinions and views (gathered informally)
- Discussions with parents

Scope of the policy:

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school. The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy / Staff Code of Conduct. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will inform parents / carers of incidents of inappropriate Online Safety behaviour that take place both within school and outside of school in line with school behaviour policy.

Roles and responsibilities of the school community:

Governors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Committee receiving information about e-safety incidents and monitoring reports through the heads report and by the eSafety Leader attending Governor meetings. **Longmeadow's School's designated eSafety Governor is Scott Dowell .**The role of the E-Safety Governor / Director will include:

- meetings with the eSafety Leader
- have an awareness of e-safety incident logs through meeting with the schools eSafety coordinator
- knowledge of filtering

Headteacher:
- The Headteacher has a duty of care for ensuring the safety (including eSafety) of members of the school community, though the day to day responsibility for eSafety will be delegated to the eSafety Leader
- The Headteacher and the SLT should be aware of the procedures to be followed in the event of a serious eSafety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / other relevant body disciplinary procedures). SWGfL BOOST includes an 'Incident Response Tool' that steps (and forms to complete) any staff facing an issue, disclosure or report, need to follow. This can be downloaded at http://www.swgfl.org.uk/Staying-Safe/E-SafetyBOOST/Boost-landing-page/Boost-Hub/Incident-Response-Tool
- The Headteacher is responsible for ensuring that the eSafety Leader and other relevant staff receive suitable training to enable them to carry out their eSafety roles and to train other colleagues, as relevant.
- The Headteacher manages the CPOMs reporting system ensuring that the eSafety Leader and all staff have a system in place to allow for monitoring and support of the internal e-safety monitoring.

Lead eSafety Coordinator:
- The lead eSafety Leader at Longmeadow is ***Catherine Badesha (Maternity Leave),*** *in her absence* ***Mr Lee Geer*** *will be the acting eSafety Leader.*
- Is a trained DSL
- takes day to day responsibility for eSafety issues and has a leading role in establishing and reviewing the school eSafety policies / documents

- ensures that all staff are aware of the procedures that need to be followed in the event of an eSafety incident taking place.
- provides training and advice for staff
- liaises with Herts for Learning and HCC when necessary
- liaises with school technical staff
- creates reports of e-safety incidents using CPOMs and creates a log of incidents to inform future eSafety developments
- meets regularly with eSafety Governor to discuss current issues and review incident logs
- attends relevant Governor meetings
- reports regularly to headship team
- Organises and runs eSafety week

InTerm IT School Technician:

- Our IT technician is ***Angelo DeLuca. InTerm IT*** is responsible for ensuring:
- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required eSafety technical requirements and any HCC or any other relevant body eSafety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with eSafety technical information in order to effectively carry out their eSafety role and to inform and update others as relevant
- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the eSafety Leader or Headteacher for investigation
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

- are responsible for ensuring that:
- they have an up to date awareness of eSafety matters including PREVENT and radicalisation (and the was technology can be used to support this) and of the current school eSafety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy ***(Appendix One.)***
- they report any suspected misuse or problem to the eSafety Leader or member of the headship team for investigation
- all digital communications relating to school matters between any member of the school community (including parents/carers) or other professionals should be on a professional level and only carried out using official school systems and through your school email address
- eSafety issues are embedded across all aspects of the curriculum and other activities
- pupils understand and follow the eSafety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead for Child Protection (DSL's):

DSL's should be trained in eSafety issues and be aware of the potential for serious 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

(NB. it is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop. It is for this reason that Assistant Head Lee Geer who is also a DSL is Longmeadow school's eSafety Leader.)

- Should an eSafety related safeguarding incident occur then the eSafety Leader should be contacted for advice.
- If an serious eSafety incident occurs then Herts for Learning should be contacted for advice.

Pupils:

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

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local eSafety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good eSafety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website
- their children's use of web based resources such as social media and the removal of accounts when children are underage

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: **child protection, health and safety, home–school agreements, and behaviour policy including anti-bullying and Values Education including the teaching of British Values.**

Policy Statements eSafety in the curriculum

New technologies and online resources are increasingly used across the curriculum. However, their use must be balanced by educating pupils to take a responsible approach. We believe that it is for eSafety guidance to be given to pupils on a regular and meaningful basis. The education of pupils in eSafety is therefore an essential part of the school's safeguarding provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and

build their resilience. This is supported throughout the school by embedding eSafety teaching into computing lesson and throughout all opportunities to use new technologies across the curriculum. We believe that eSafety is fully embedded across our curriculum and that staff continually look for new opportunities to embed, promote and develop eSafety provision.

At Longmeadow we believe that eSafety should be a focus in all areas of the curriculum and staff should consistently reinforce eSafety messages at all times. The eSafety curriculum is embedded within the computing curriculum and represents a broad, relevant and progressive understanding, with opportunities for creative activities and will be provided in the following ways:

- A planned eSafety curriculum is provided as part of Computing and is regularly revisited
- Educating pupils on the dangers of technologies is completed informally when opportunities arise alongside the planned eSafety curriculum
- Key eSafety messages are reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils are 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 are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are aware of the impact of cyber bullying and how to seek help if they are affected by these issues in line with the anti-bullying policy.
- Students / 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. Staff should report any concerns using the PREVENT lozenge on CPOMs.
- Pupils are made aware of what to do when they face challenges online (I.e. tell a trusted adult, report to the website etc)
- Staff act as good role models in their use of digital technologies the internet and mobile devices when modelling their use to children including during lessons
- in lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

eSafety

Education:

Education – parents / carers

At Longmeadow we believe that parents / carers play an essential role in the promotion of eSafety. We accept that parents/carers 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. We regularly consult and discuss eSafety with parents / carers and seek to promote a wide understanding of the benefits and risks associated with the use of new technologies for children.

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

- Weekly National Online Safety bulletin #WakeUpWednesdays is published on the school website
- Letters, newsletters, website and school Facebook page
- Parents / Carers evenings / sessions
- High profile events / campaigns eg eSafety week including parent workshop run curriculum activities

- Encouragement to share their views on eSafety through annual parent view survey and monthly parent forum
- Reading and signing of the acceptable use agreement on behalf of their child before admission to school • Consent regarding the use of children's images being taken / used in the public domain (i.e.
  on the school website or blog)

Education – The Wider Community

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

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety
  - E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide e-safety information for the wider community
- Supporting community groups eg Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their e-safety provision. This includes the support of other local schools by the eSafety Leader.
- Liaising with the local police to provide support to the school and / or parents.

Education & Training – Staff / Volunteers

At Longmeadow we view the annual staff e-safety training as essential and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training is made available to staff through memos and a termly computing staff meeting. This is regularly updated and reinforced. An audit of the eSafety training needs of all staff is carried out regularly. It is expected that some staff will identify eSafety as a training need within the performance management process.
- All new staff receive eSafety training as part of their induction programme, ensuring that they fully understand the school eSafety policy and Acceptable Use Agreements.
- The eSafety Coordinator is a trained CEOP ambassador and trainer and receives regular updates relating to eSafety through attendance at external training events (eg Herts for Learning, RM Education, CEOP) and by reviewing guidance documents released by relevant organisations.
- This eSafety policy and its updates are presented and discussed by staff in staff / phase meetings / INSET days.
- The eSafety Coordinator provide advice / guidance / training to individuals as required and identified by the individual.
- All staff to receive an annual PREVENT update to ensure they have an appropriate level of knowledge surrounding Prevent, radicalisation and FGM. This will be run by the lead DSL and the eSafety Leader who will highlight the role technology can play in selection and grooming.

Education – Governors

There is a dedicated governor for eSafety at Longmeadow. Governors take part in eSafety training. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (eg SWGfL).
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).
- Training from the eSafety Leader at Governor meetings

- Governors are presented with and expected to sign the acceptable use policy.
- Governors can identify the need for further support / training with the eSafety Leader on an individual basis if necessary

Managing the school eSafety Message

We believe strongly in promoting our eSafety message at all times. Children need to hear eSafety messages consistently. We will promote the schools eSafety message by:

- embedding eSafety messages across the curriculum whenever new technologies or online resources are used
- Relevant parts of the eSafety policy are introduced to the children at the beginning of the year and continually embedded throughout the year
- Children will be made continually aware of the school reporting slogan ***"before you click, you need to think and tell someone!"***
- eSafety posters are prominently displayed throughout the year
- The school eSafety group will run each year with new pupil members selected at the start of each academic year
- The eSafety group will think of exciting ways to engage pupils with new technologies and eSafety such as competitions etc

Technical – infrastructure / equipment, filtering and monitoring

Longmeadow has a managed ICT service provided by an InTerm IT in conjunction with LARA. It is the responsibility of the school to ensure that our service providers carry out all the eSafety measures. The persons responsible for this are Will and Angelo. InTerm IT are fully aware of the school eSafety Policy and Acceptable Use Agreements. The school policy is written in consultation with Herts for Learning and South West Grid for Learning template policies.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements (these may be outlined in Local Authority / other relevant body policy and guidance)
- 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 pupils will be provided with a username (format year of admission, first name, initial of surname) and secure password (from KS2) by the school technician who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "administrator" passwords for the school system, used by the Network Manager (or other person) must also be available to the Headteacher and the new technologies Leader and kept in a secure place (eg school safe)
- The headteacher and new technology Leader 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 (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- The school understands its duty to keep children safe by filtering its internet services. The internet into school is filtered for all users through the LA's web filtering service 'the grid'. For further information relating to filtering please go to http://www.thegrid.org.uk/eservices/safety/filtered.shtml
- The school provides differentiated user-level filtering (allowing different filtering levels for different groups of users – staff / pupils). We have staff on WF1 and pupils on WF3

- **WF3** is ideally suited for primary school children. YouTube and social networking sites such as Facebook are blocked. You will also find that restrictions are in place, denying access to non-educational games websites.
- **WF1** is the least restrictive and can therefore be regarded as our baseline policy, being geared towards trusted users such as staff. It denies access to pornography, the promotion of illegal activities and to the propagation of hatred but most other material is allowed. Staff understand that their workstation must be locked when not in use as stated in the staff acceptable use agreement.
- The school also understands that Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet under the Counter Terrorism and Securities Act 2015 which requires schools / academies to ensure that children are safe from terrorist and extremist material on the internet.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Reports of any actual / potential technical incident / security breach should be reported directly to Catherine Badesha and InTerm Technician(s).
- 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 provided by the grid.
- Temporary access of "guests" is accessed through the use of supply log ins to the system (eg trainee teachers, supply teachers, visitors) onto the school systems. The use of these should be monitored by the member of staff working with this person.
- Staff should contact Catherine Badesha or InTerm Technician(s) regarding for the downloading and installing of programs onto the school network or school devices. This should only be completed with permission from the new technologies Leader.
- The use of removable media (eg memory sticks / CDs / DVDs) by users on school devices is permitted. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. These passwords must contain a character and number to increase security. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- The main administrative machines and the head's machine, which hold personal data of children & staff, have their passwords changed termly.
- Staff change their passwords a minimum of annually. The new technologies Leader can administer a password reset for all staff via the server if deemed necessary.
- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's eSafety Policy.
- Users are provided with an individual network and email username and password.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.

- If you think your password may have been compromised or someone else has become aware of your password report this to Lee Geer and InTerm Technician(s).
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks and MIS systems including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic log-off time for the school network is 1 minute.
- In our school, all ICT password policies are the responsibility of InTerm Technician(s) and all staff and pupils are expected to comply with the policies at all times.

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

- When using digital images, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use 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 *students / pupils* in the digital / video images. This message will be delivered by a member of the headship team at the start of any such event.
- 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.
- Photographs published on the website, or elsewhere that include students / pupils will be selected in relation to photo consent gained from parents / carers annually.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website (may be covered as part of the photograph consent form signed by parents or carers at the start of the year - see Parents / Carers acceptable Use Agreement in the appendix)
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which 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 ensures 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". (see Privacy Notice section in the appendix)
- It has a Data Protection Policy (see appendix for template policy)
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Miss M Flanagan and Ms P Flint (DPO)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

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. This is created through password protected access to the network.
- 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.
- Members of the headship team and senior leadership team access the school network through the LARA. This is a secure method to access the network remotely when offsite and is provided by InTerm.

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 once it has been transferred or its use is complete

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the **Hertfordshire Grid for Learning** (HGfL) is logged and the logs

are randomly but regularly monitored. Whenever any inappropriate use (as defined in HCC Guidance for Safer Working Practice) is detected it will be followed up.

- The school maintains students will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology. Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Managing other Web 2 technologies

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking sites to pupils within school.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the school.
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using the LA Learning Platform or other systems approved by the Headteacher.
- If children are accessing social media beyond their age remit then their parents must be immediately informed and asked to remove the profile. If this does not happen parents must meet with Catherine Badesha and new technologies Leader who will again re-iterate the need for the profile to be removed. If after one week this has not happened the site (I.e. Facebook) will be contacted correctly and the profile will be reported, asked to be removed with the child's correct date of birth.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit

and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device, apart from when schools are expected to provide remote education (National Lockdowns etc). At this time, staff should only use their personal mobile when withholding their number. Personal devices are NEVER to be used by staff in the presence of children. This includes the use of SMART watches (i.e. Apple watches)
- Pupils are not currently allowed to bring personal mobile devices/phones to school. If this is required for safety when walking to and from school independently in Y5/6 then the phone is to be handed into the school office.
- Pupils are not allowed to have a personal device on their person in school. This includes the use of SMART watches.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices (including phones)

- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.
- Permission should be sought from the phase leader before these devices are taken off of school site.
- Devices must be set to the school password to protect children's images when offsite (i.e. on a school trip).

Managing email

The use of email within most schools is an essential means of communication for both staff, pupils and governors. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette' and emails presence in the Computing curriculum.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- The school requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending emails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated account.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- All children use a class/ group email address under the direct supervision of the teacher.
- The forwarding of chain letters is not permitted in school. However the school has set up a dummy account (***dummy@Longmeadow.herts.sch.uk***) to allow pupils to forward any chain letters causing them anxiety. This account will not be used by any member of the school community, other than to monitor inappropriate emails.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform (the eSafety Leader/ line manager) if they receive an offensive email.
- Pupils are introduced to email as part of the Computing Scheme of Work.

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. While, Ofsted's online safety inspection framework reviews how a school protects and educates staff and pupils in their use of technology, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, 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 limiting access to personal information:

- Training includes: acceptable use; social media risks; checking of settings; data protection; reporting issues; prevent duty
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the headship team and eSafety committee.

Webcams and CCTV

- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes.
- At times specific learning videos are posted on the school website as a VLOG. These also appear on the school Facebook page. Explicit consent is sought from parents before this happens.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)

    - Webcams can be found on iPad devices and iPod touch devices. Notification is given in this/these area(s) filmed by webcams by signage.
    - Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.

For further information relating to webcams and CCTV, please see
http://www.thegrid.org.uk/schoolweb/safety/webcams.shtml

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.
- All pupils are supervised by a member of staff when video conferencing
- All pupils are supervised by a member of staff when video conferencing with end-points beyond the school.
- The school keeps a record of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school.
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the consent of those taking part.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

For further information and guidance relating to Video Conferencing, please see
http://www.thegrid.org.uk/learning/ict/technologies/videoconferencing/index.shtml **Misuse and Infringements**

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school / academy 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 Page 33 would be inappropriate in a school /academy context, either because of the age of the users or the nature of those activities. The school / academy believes that the activities referred to in the following section would be inappropriate in a school / academy context and that users, as defined below, should not engage in these activities in / or outside the school / academy when using school / academy equipment or systems. The school / academy policy restricts usage as follows:

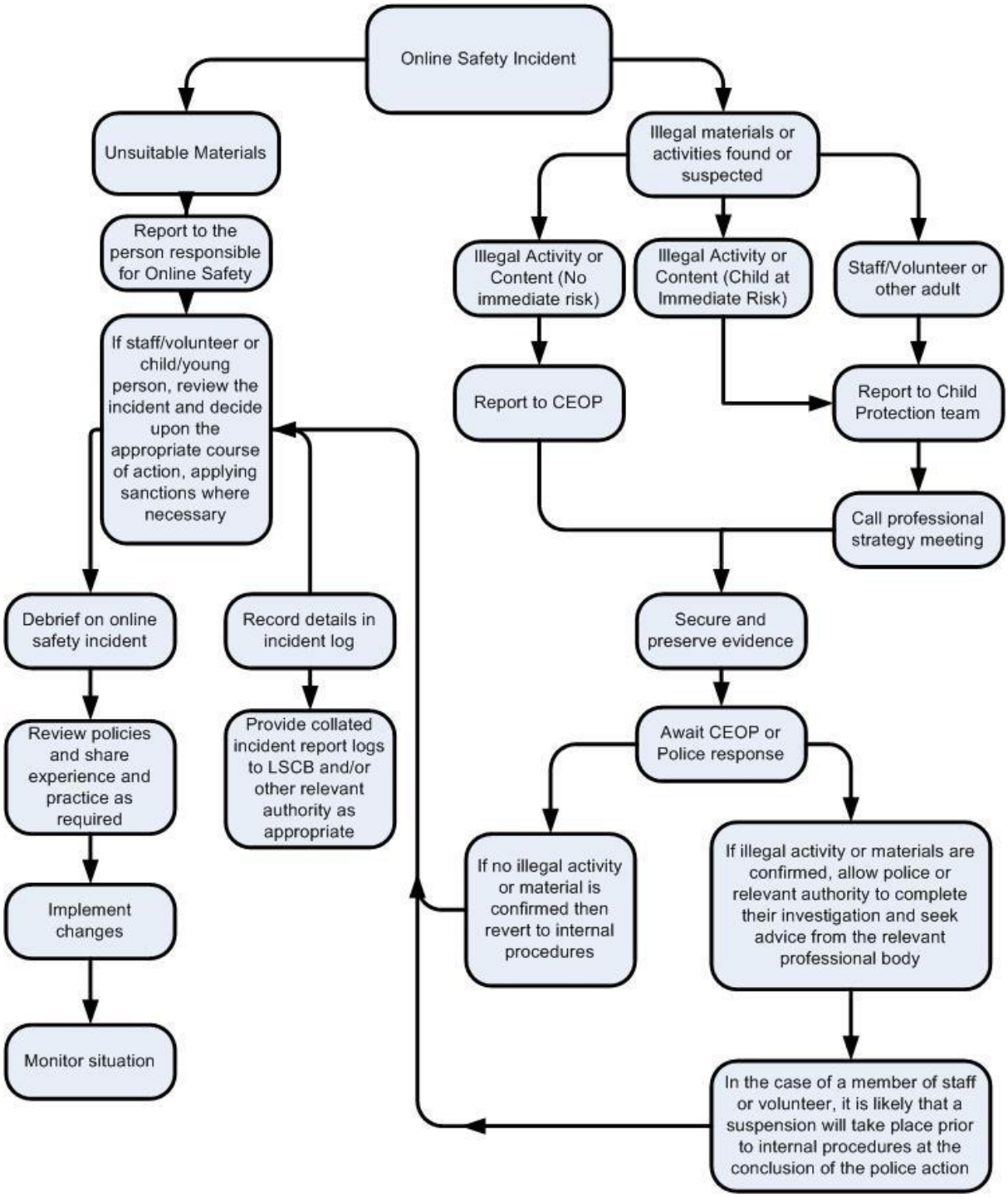
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites.	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	

User Actions

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

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, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour ○ the sending of obscene materials to a child ○ adult material which potentially breaches the Obscene Publications Act ○ criminally racist material ○ promotion of terrorism or extremism ○ 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 / academy and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

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

Actions / Sanctions

Students / Pupils Incidents	Refer to class teacher / tutor	Refer to Head of Department / Year / other	Refer to Headteacher / Principal	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 eg 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
Unauthorised use of non-educational sites during lessons	X								X
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device		X				X			X
Unauthorised / inappropriate use of social media / messaging apps / personal email		X				X		X	X
Unauthorised downloading or uploading of files		X				X		X	X
Allowing others to access school / academy network by sharing username and passwords	X					X		X	X
Attempting to access or accessing the school / academy network, using another student's / pupil's account	X					X		X	X
Attempting to access or accessing the school / academy network, using the account of a member of staff		X	X			X	X		X
Corrupting or destroying the data of other users	X					X	X		X
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		X	X		X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school		X	X			X			X

Using proxy sites or other means to subvert the school's / academy's filtering system									
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	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

Staff

Actions / Sanctions

Staff Incidents	Refer to line managerr	Refer to Headteacher	Refer to Local Authority / Principal	Refer to Police HR	Refer to Technical Support Staff for action re filtering	Warning etc	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		
Unauthorised downloading or uploading of files	X	X			X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X					X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X				X		
Deliberate actions to breach data protection or network security rules	X	X						X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X				X		

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

Complaints

Complaints relating to eSafety should be made to the eSafety Leader or Headteacher. Incidents should be logged via CPOMs under the eSafety category and the SWGfL Flowcharts for Managing an eSafety Incident should be followed (see appendix).

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety Leader.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety Leader, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart.)
- Users are made aware of sanctions relating to the misuse or misconduct in the relevant policy documents.

Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules.
However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

ACKNOWLEDGMENTS

This policy has been written to support the safety of the pupils at Longmeadow Primary School. Advice has been taken from Herts for Learning and South West Grid for Learning and this policy has been modelled upon their templates whilst being modified and personalised to ensure that it is fit for purpose for the all members of the school community.

APPENDIX ONE – STAFF ACCCEPTABLE USE AGREEMENT

ACCEPTABLE USE AGREEMENT: STAFF, GOVERNORS AND VISITORS

ACCEPTABLE USE AGREEMENT / CODE OF CONDUCT

ACCEPTABLE USE AGREEMENT: STAFF, GOVERNORS AND VISITORS

ACCEPTABLE USE AGREEMENT / CODE OF CONDUCT

Computing and the use of related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of new technology. All staff are expected to read this agreement and sign the staff declaration as part of safeguarding. Staff should adhere to the contents of this acceptable use policy at all times. Any concerns or clarification should be discussed with *Catherine Badesha* the schools eSafety coordinator.

- I will only use the school's email / Internet / Intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with all new technologies security. This includes ensuring all technology within the school is stored securely at all times.
- I will not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils or parents.
- I will only use the approved, secure school email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. This is through the use of the VPN or an encrypted memory stick available from the eSafety coordinator.
- I will not install any hardware of software. I will instead gain the permission of the New Technologies coordinator and then add this to the InTerm IT technician's job sheet.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will ensure my workstation is locked at any time I am not working at it to ensure it cannot be accessed by a child.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. This includes my use of social media.
- I will support and promote the school's eSafety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will not use personal electronic devices (including smart watches) in the presence of children.

Users to read acceptable use agreement as part of the child protection policy. Staff sign Appendix 2: Declaration for staff to state that they have read and understood the schools acceptable use agreement. Signing this declaration also states that you agreed to adhere to the acceptable use agreement at all **times.**

APPENDIX TWO –PUPIL ACCEPTABLE USE AGREEMENT

Dear Parents

Responsible Internet Use

As part of your child's curriculum and the development of computing skills, Longmeadow Primary School provides access to the internet. At Longmeadow Primary School we have an eSafety policy which I would like to summarise for you.

We believe that the effective use of the internet and email is an essential skill for children as they grow up in the modern world. The internet is an important element in 21st century life for education, business and social interaction. As a result, the school has a duty to provide students with quality internet access as part of their learning experience.

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. We take internet safety very seriously in school and only access the internet through the local authority intranet, which is subject to strict controls and monitoring. This means that inappropriate sites and images are filtered out before they ever get to the school computers, creating a very safe zone for children to work in at school.

We therefore take all reasonable precautions to ensure that users access only appropriate material. Despite this, due to the international scale and linked nature of internet content, it is not possible to completely guarantee that unsuitable material will never appear on a school computer.

We have decided to operate an opt out agreement. Please would you read the attached Rules for Responsible Internet Use. If you do not agree to abide by the statements then please sign to opt out and this will be discussed with you by Catherine Badesha (eSafety Leader), and myself. If you do not opt out you also agree that your child may use internet at school and have their work published on the internet.

Should you wish to discuss any aspect of internet use, please telephone me to arrange an appointment.

Emily Howley

Headteacher

Responsible Internet Use

These rules help us to be fair to others and keep everyone safe.

- My child will ask permission before using the Internet.
- My child will use their own login and password.
- My child will only look at or delete their own files.
- My child will not bring software, disks or memory sticks into school without permission.
- My child will only email people they know, or who their teacher has approved.
- The messages my child sends will be polite and sensible.
- My child understands that they must never give their home address or phone number, or arrange to meet someone.
- My child will ask for permission before opening an email or an email attachment sent by someone they do not know.
- My child will not use internet chat whilst in school.
- If my child sees anything they are unhappy with or they receive messages they do not like, I will encourage my child to report this to an adult immediately.
- I understand that the school may check my child's school log in for files and the internet sites they visit.
- I understand that if my child deliberately breaks these rules, they may not be allowed to use the internet or computers.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. This includes evidence of extremism or radicalisation.

Parents & Carers:

I/we will ensure that my/our online activity would not cause the school, staff, pupils or others distress or bring the school community into disrepute.

I/we will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset or offend any member of the school community.

I/we will support the school's policy and help prevent my/our child/children from signing up to services such as Facebook, Instagram, Snapchat and YouTube whilst they are underage (13+ years in most cases).

I/we will close online accounts if I/we/teachers find that these accounts are active for our underage child/children.

APPENDIX THREE –FLOWCHARTS FOR MANAGING AN E-SAFETY INCIDENT

Hertfordshire Flowchart to support decisions related to an Illegal eSafety Incident

For Headteachers, Senior Leaders and eSafety Coordinators

Following an incident the eSafety Coordinator and/ or Headteacher will need to decide quickly if the incident involved any illegal activity

If you are not sure if the incident has any illegal aspects contact immediately for advice either:
Herts. ICT Technical Adviser 01438844809 or Police Referrals Unit 01707 355913

Illegal means something against the law such as:
- Downloading child pornography
- Passing onto others images or video containing child pornography
- Inciting racial or religious hatred
- Promoting illegal acts

Was **illegal** material or activity found or suspected?

Yes

1. Inform police and the Herts. ICT Technical Adviser. Follow any advice given by the Police otherwise:
2. Confiscate any laptop or other device and if related to school network disable user account
3. Save **ALL** evidence but **DO NOT** view or copy. Let the Police review the evidence

☏ If a pupil is involved inform the Child Protection School Liaison Officer (CPSLO) on 01992 556936.
☏ If a member of staff contact the Local Authority Designated Officer for Allegations Management (LADO) on 01992 556935.

No

If the incident **did not** involve any **illegal activity** then follow the **next flowchart** relating to non-illegal incidents

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to a member of staff or the eSafety Coordinator

---

If the incident **did not** involve **any illegal activity** then follow this flowchart

Hertfordshire Managing an eSafety Incident Flowchart

For Headteachers, Senior Leaders and eSafety Coordinators

The eSafety Coordinator and/ or Headteacher should:
- Record in the school eSafety Incident Log
- Keep any evidence

Incident could be:
- Using another persons user name and password
- Accessing websites which are against school policy e.g. games
- Using a mobile phone to take video during a lesson
- Using the technology to upset or bully (in extreme cases could be illegal) – talk to Herts. Anti-Bullying Adviser Karin Hutchinson 01438 844044

Did the incident involve a member of staff?

Yes

If member of staff has:
1. Behaved in a way that has, or may have harmed a child.
2. Possibly committed a criminal offence.
3. Behaved towards a child in a way which indicates s/he is unsuitable to work with children.

Contact the LADO on: 01992 556935

If the incident **does not** satisfy the criteria in **10.1.1** of the **HSCB procedures 2007**, then follow the bullet points below:
- Review evidence and determine if the incident is accidental or deliberate
- Decide upon the appropriate course of action
- Follow school disciplinary procedures (if deliberate) and contact school HR Sandie Abery 01992 555911 South-E Rachel Hurst 01992 555841 North-W

No

Was the child the victim or the instigator?

Pupil as victim

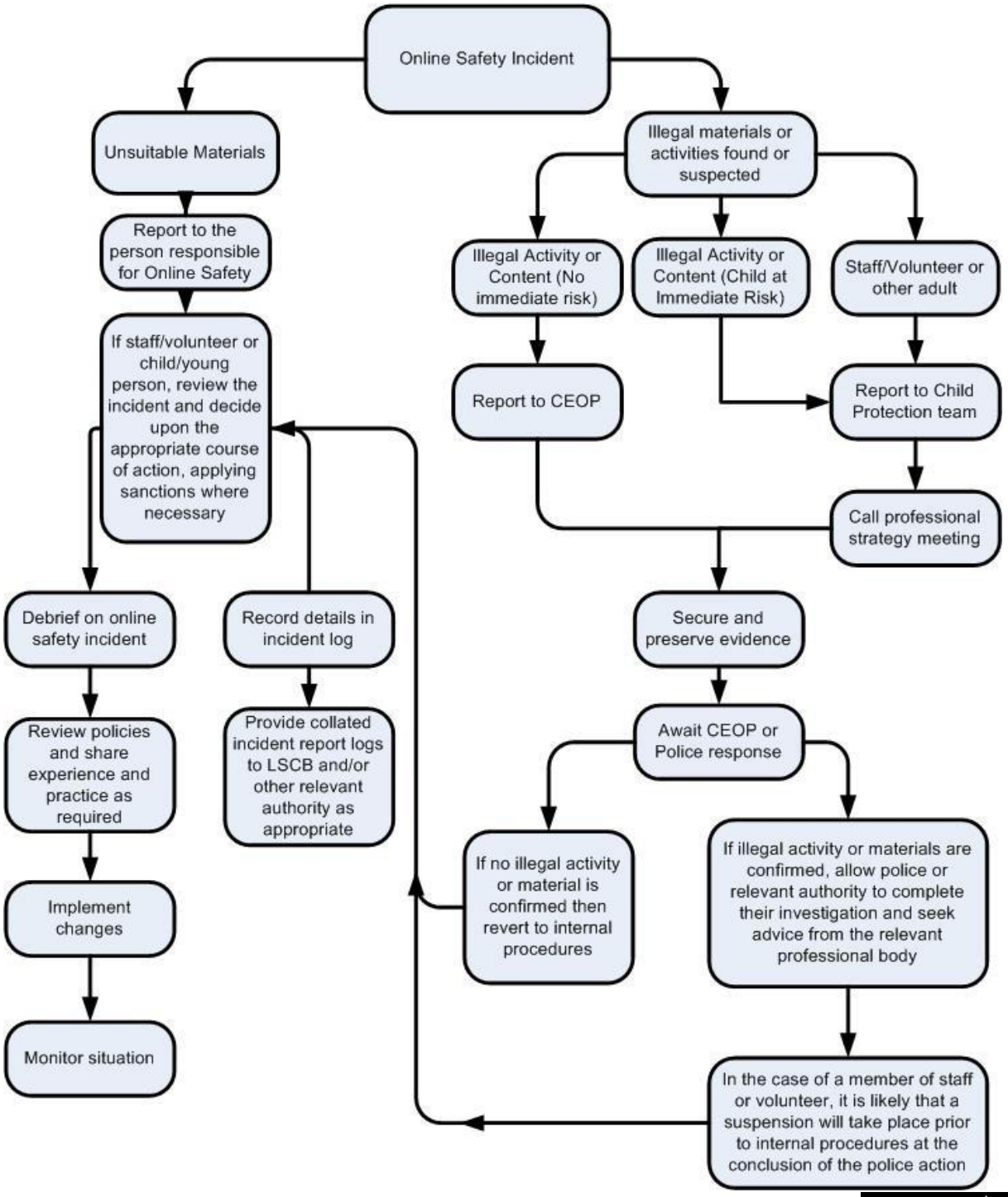
In –school action to support pupil by one or more of the following:
- Class teacher
- eSafety Coordinator
- Senior Leader
- Headteacher
- Designated Senior Person for Child Protection (DSP)

Inform parents/ carer as appropriate
If the child is at risk inform CSPLO immediately

Pupil as instigator

- Review incident and identify if other pupils were involved
- Decide appropriate sanctions based on school rules/ guidelines
- Inform parents/ carers if serious or persistent incident
- In serious incidents consider informing the CPSLO as the child instigator could be at risk
- Review school procedures/ policies to develop best practice

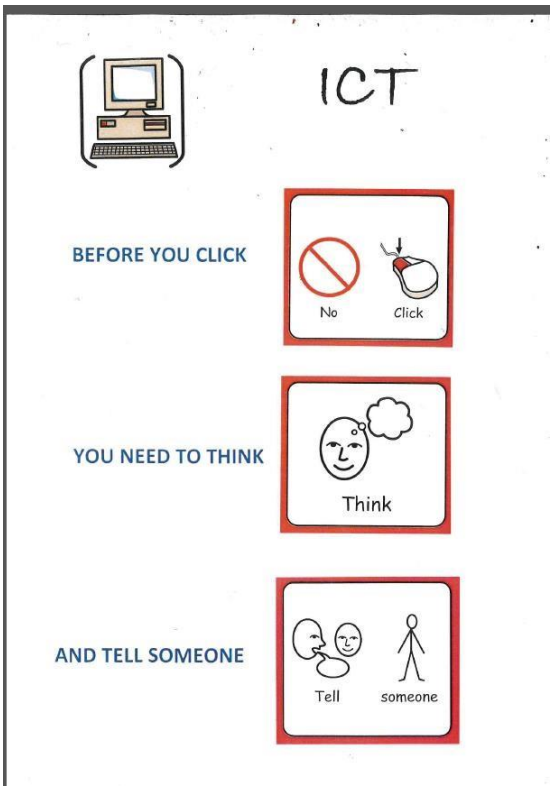
Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and talk to a member of staff or the eSafety Coordinator

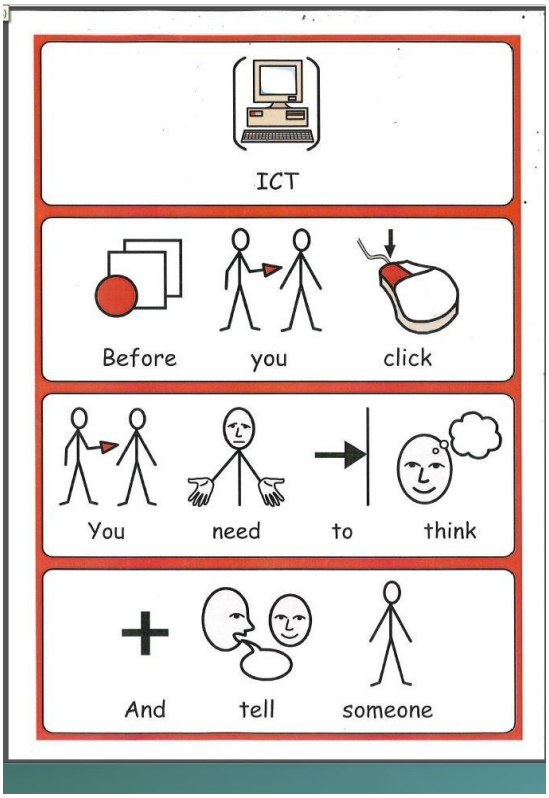


APPENDIX FOUR: e-Safety Incident Log

All eSafety incidents are now logged via CPOMs.

APPENDIX FIVE: School eSafety Posters





APPENDIX SIX: Legislation

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online. It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities; • Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system; • Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003
A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression

- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006
Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011
Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012
Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012
Requires schools to publish certain information on its website: https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015
Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

APPENDIX SEVEN: Advice to Parents/Carers supporting pupils with remote learning

- **Screen time**

  Consider the amount of time that children are sitting down accessing online activities and help them plan their days to include non-digital activities such as time outside, exercise, and creativity. Keeping a diary of daily learning in all its forms and including the skills they are using will be useful for their wellbeing and sense of achievement.

  https://www.childnet.com/ufiles/Young-children-and-screen-time---a-guide-for-parents-and-carers.pdf

- **Setting up parental controls and privacy settings**

  Parental controls can help you control the content your child can see or experience online. Internet matters offer a suite of straightforward step by step guides to help set up the right controls and privacy settings on different networks, devices, apps and sites. This site can be accessed here: https://www.internetmatters.org/parental-controls/

- **Regular conversations about online safety**

  Parental controls and privacy settings are useful tools to help minimise the risks children may face but they can never be totally effective. Always encourage your child to come and talk to you if they find anything that upsets them online. The NSPCC and O2 Net Aware have published a useful guide on starting a conversation about online safety. Visit the website for further information:

  https://www.nspcc.org.uk/keeping-children-safe/online-safety/talking-child-online-safety/

- **A balanced diet online!**

  Encourage children to have a good digital diet which includes a balance of being connected to others, seeking ideas for active and creative activities, focusing on how they can give to others and being mindful. The digital 5 a day: A guide for children and young people can be accessed here: https://www.childrenscommissioner.gov.uk/our-work/digital/5-a-day/

- **Importance of good sleep**

  Try to ensure children have at least an hours break from looking at a screen before bedtime and that mobile devices stay out of bedrooms at night. Ensuring efficient physical activity during the day will also aid a good night's sleep. It is recommended by Public Health England (PHE) that children have at least an hour's rigorous activity per day. You may wish to consider maintaining the 'Daily Mile' as a family while maintaining your distance from others who may also be outdoors.

- **Keeping personal information safe**

  Remind young children not to share personal information such as name and contact details with others online.

- **Help children think critically about online content**

Remind children that not everything we read or see on the web is true and not everyone online tells the truth.

- **Know who they are talking to online**

  Social media and gaming. Regularly ask children who they are talking to online and ensure that they are only speaking with people they know in the real world. Ensure that children understand that if anyone they don't know makes contact with them then they must come to tell you. It is important they know you will help them block that contact.

  Other useful websites include:

  www.gooseberryplanet.com/safeguarding-during-school-closures-due-to-the-corona-outbreak-parent-advice/

  www.parentinfo.org/

  www.saferinternet.org.uk

  www.thinkuknow.co.uk

  www.swgfl.org.uk/resources/checklists

This is also an important time to do things together as a family that are not technology related such as:

- A visit to the local park. The National Trust are opening many of its parks and gardens for free to encourage everyone to enjoy open spaces whilst adhering to the government's social distancing guidance.
- Starting a family group read with a favourite book, taking it in turns to read to each other
- Listening to a range of different music or singing together
- Healthy cooking projects
- Having a family jigsaw on the go and playing board games
- The 'Change for Life Activities' website has lots of further suggestions https://www.nhs.uk/change4life/activities

APPENDIX Eight: Working from home guidelines for staff

Due to the current COVID-19 situation, staff in many school and settings will be working remotely from home. Potential risks and how to overcome these are listed below.

• Only a school or setting device may be used to conduct school business at home. (The only exception would be where a closed, monitor able system (LARA) has been set up by the school for use on a personal device. Such a system would ensure the user was not saving files locally to their own device and breaching data security.) Any deviation from this to use a home owned device when working from home would need specific written approval /risk assessment from the Headteacher and safeguarding lead.

• Always ensure a device has been locked or logged off when left unattended to prevent sensitive data being accessed by others. Such data could be unwittingly accessed, changed, copied or forwarded.

• Do not use a device where it can be overlooked by unauthorised persons and do not leave it unattended in public places.

• Do not allow family and friends to use school devices.

• Staff must preview sites, software and apps before recommending them to pupils to access at home.

• Staff must only use pre-approved school and setting systems if creating blogs, wikis or other online areas in order to communicate with pupils/ families.

• Staff should not contact pupils, parents or conduct any school or setting business using a personal email address.

• Ensure that you know who to report to if your school or setting device is lost or stolen. Reports of loss or theft should be made as soon as possible.

• Staff required to make a conference call to other staff or pupils should be fully appraised of how to use the technology. These communication processes should have been risk assessed (including parental home learning agreements where appropriate).