VALLEY PRIMARY SCHOOL

E-Safety
Policy
May 2021

This policy explains how we aim to protect and support children when they are using technology to support their education, within school and within the wider community.

The 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 e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Contents

Development, monitoring and review of the policy
Schedule for development, monitoring and review
Scope of the policy

Roles and Responsibilities
- Governors
- Headteacher and senior leaders
- Safeguarding designated person (E-safety lead)
- Teaching and support staff
- Child protection/Safeguarding designated person
- E-Safety Committee
- Pupils
- Parents/carers
- Community users

Policy Statements
- Education – Pupils
- Education – Parents/carers
- Education – The wider community
- Education and training – Staff/volunteers
- Training – Governors
- Technical – infrastructure/equipment, filtering and monitoring
- Bring your own devices (BYOD)
- Use of digital and video images
- Data protection
- Communications
- Social media - Protecting professional identity
- User actions - unsuitable/inappropriate activities
- Responding to incidents of misuse

Appendices:
- Pupil Acceptable Use Policy Agreement template – older children (KS2)
- Pupil Acceptable Use Policy Agreement template – younger children (KS1)
- Legislation
- Links to other organisations and documents

Development /Monitoring/ Review of this policy

This e-safety policy has been developed by with input from all users and 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 Governing Body* on:	*May 2021*
The implementation of this e-safety policy will be monitored by the:	*Head Teacher and Computing Subject leader*
Monitoring will take place at regular intervals:	*Annually*
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:	*Annually*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.	*May 2022*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Board, Police*

The school will monitor the impact of the policy using:
- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys/questionnaires of
  - students/pupils
  - parents/carers
  - staff

Roles and responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school.

Governors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. A member of the Governing Body has taken on the role of Safeguarding Governor. This role will include:

- regular meetings with the E-Safety Lead
- regular monitoring of e-safety incident logs
- regular monitoring of filtering/change control logs
- reporting to full Governing Body meetings

Head Teacher and Senior Leaders:

- The Head Teacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Lead.
- The Head Teacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Head Teacher/Senior Leaders are responsible for ensuring that the E-Safety Lead and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Head Teacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. This will normally be at a regular meeting with additional support as required. It is noted that the Whistleblowing Policy may be relevant in some cases.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Lead.
- The Head Teacher, in consultation with the Trust's Head of Compliance and the school's IT provider (TurnItOn), will ensure that the appropriate level of security is place to minimise the potential of acts of cyber crime including ransomware and cyber attackes being carried out on the school systems

Role of the E-Safety Lead (Responsibility of Safeguarding Designated Person)

- Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e- safety incident taking place.
- Provides training and advice for staff.
- Liaises with Bromley Safeguarding Board.
- Liaises with technical staff and IT support suppliers.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments, meets regularly with the Safeguarding Governor to discuss current issues, review incident logs and filtering/change control logs.
- Attends relevant meeting/committee of Governor.
- Reports regularly to Senior Leadership Team.

Computing Lead, teaching and support staff

are responsible for ensuring that:
- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- they have read, understood and signed the Staff Acceptable Use Agreement (AUA);
- they report any suspected misuse or problem to the Headteacher / Senior Leader ; E-Safety Lead for investigation/action/sanction;
- all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems;
- e-safety issues are embedded in all aspects of the curriculum and other activities;
- pupils understand and follow the e-safety 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; and
- 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.

Safeguarding Designated Person

should be trained in e-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; and
- cyber-bullying.

Pupils

Pupils should understand that they:
- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy;
- need to 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;
- know and understand policies on the taking/use of images and on cyber-bullying; and
- know the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.
- Have a digital footprint and, in line with the Home-School Agreement, will act in a safe, kind and considerate manner towards fellow pupils, parents and staff both in the real and virtual worlds.

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 e-safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events;
- access to parents' sections of the website/VLE and online student/pupil records; and
- their children's personal devices in the school/academy (where this is allowed).

Community users

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

Policy Statements

Education – pupils

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

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

- A planned e-safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff and a member of the Senior Leadership Team can temporarily remove those blocked sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents/carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Parents may underestimate how often children and young people

come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:
- Curriculum activities
- Letters, newsletters, website
- Parents/carers sessions e.g an e-safety evening or information provided at parents' evenings
- High profile events/campaigns e.g Safer Internet Day
- Reference to the relevant websites/publications

Education – The wider community

The school will provide opportunities for local community groups/members of the community to gain from the school's e-safety 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; and
- supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their e-safety provision.

Education & Training – Staff/volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:
- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-safety Policy and Acceptable Use Agreements.
- The E-Safety Lead will receive regular updates through attendance at external training events (eg from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This E-Safety Policy and its updates will be presented to and discussed by staff in staff/ team meetings/INSET days.
- The E-Safety Lead/Computing Lead will provide advice/guidance/training to individuals as required.

Training – Governors

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any sub-committee involved in technology/e-safety/health and safety/child protection. 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.

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 e- safety responsibilities:

- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- Staff users have their own usernames and passwords for logging onto school computers. Students use shared year group accounts.
- The "master/administrator" passwords for the school ICT system, used by the IT support team (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe).
- TurnItOn along with their IT Support Technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users by LGFL. Illegal content (e.g. child sexual abuse images) is filtered by LGFL by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- The school has provided enhanced/differentiated user-level filtering.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed. Incidents are reported to class teachers or other members of staff, and escalated to the Network Manager (and/or Senior Leadership and Headteacher if deemed appropriate).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place as well as guest WiFi and computer logins for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed staff conduct policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed staff conduct policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Bring Your Own Device (BYOD)

This is not planned at Valley Primary School at the moment but will be reviewed regularly, assessing the benefits to learning against the potential risks.

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 should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/ made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Pupil's work can only be published with the permission of the pupil and parents or carers.

Remote Learning

The school has a separate Remote Learning Policy which clearly sets out the expectations for pupils, parents and staff when delivering lessons remotely. This policy can be found on the policy section of the school website.

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 for the purpose of which it was intended;
- processed in accordance with the data subject's rights;
- secure; and
- only transferred to others with adequate protection.

The school/academy 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.
- It has a Data Protection Policy.
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed/identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs) – Headteacher and School Business Manager.
- 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.

GDPR (2018)

When using data (including images or evidence from online activities) all Valley staff will be aware of Article 5 of the GDPR requiring that personal data shall be:

(a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes or statistical

purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

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 ;
- the device must offer approved virus and malware checking software; and
- 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.

As the school moves towards using Cloud-based storage, then the use of memory sticks or removable media should start to reduce.

NB. The Site Manager carries a mobile phone at all times to ensure availability but this is not used when children are present.

When using communication technologies the school considers the following as good practice:
- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, chat, etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Children can use email through the approved scheme email system (Purple Mash in 2021) and they can only email children in their class and the class teacher approves each email. Children will be taught to use email safely and respectfully.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate

    appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Valley Primary School acknowledges that it 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 liable to the injured party. Valley Primary School therefore has the following steps to prevent predictable harm 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 to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- Staff should not use their full names when creating social media accounts.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Be aware of advice from professional bodies, eg. NASUWT.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable/inappropriate 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 school or outside school when using school equipment or systems. The school policy restricts usage as follows: Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978.
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008.
- 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.
- Pornography.
- Promotion of any kind of discrimination.
- Threatening behaviour, including promotion of physical violence or mental harm.
- Any other information which may be offensive to colleagues or breaches the integrity of the

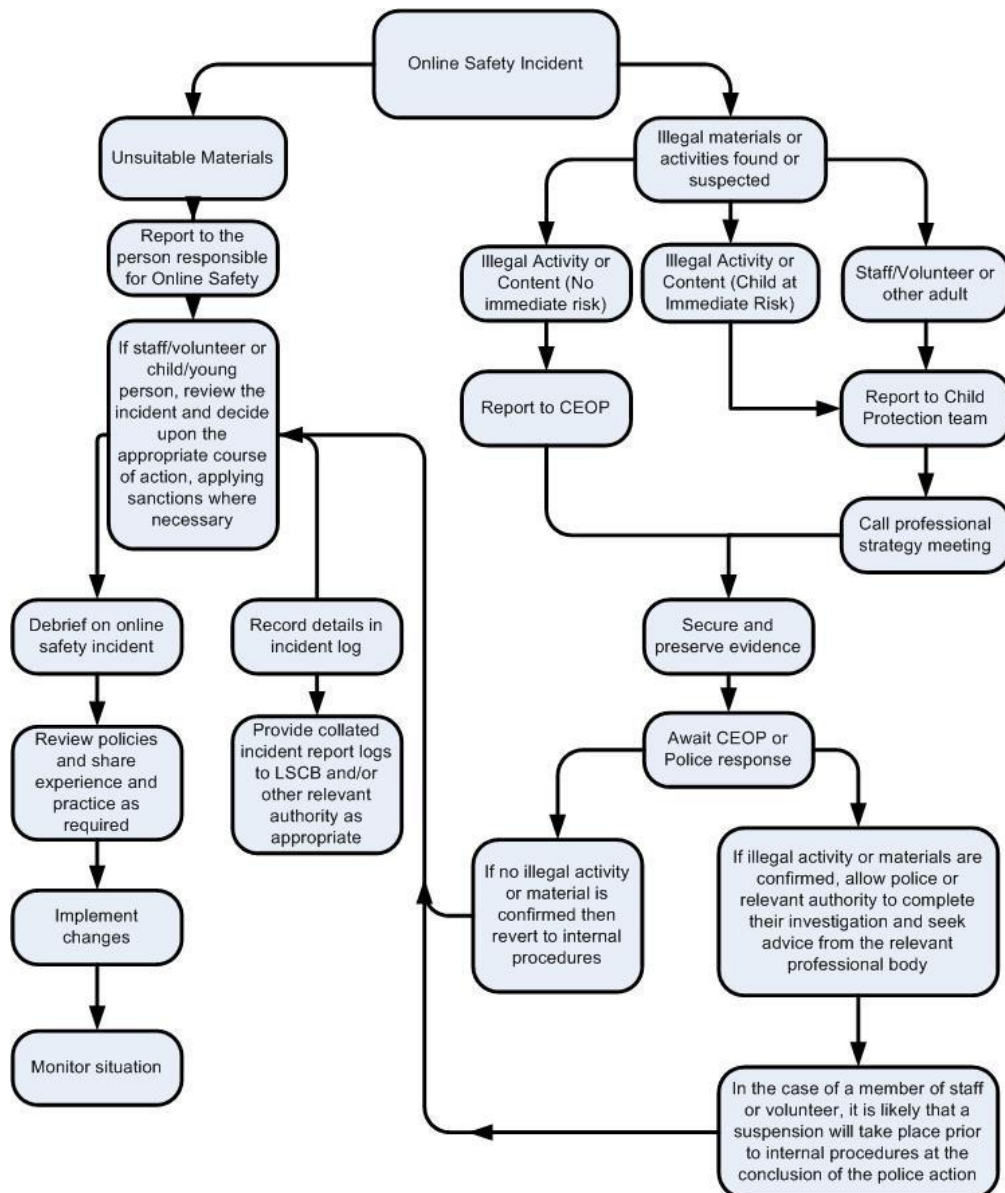ethos of the school or brings the school into disrepute.
- Using school systems to run a private business.
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy.
- Infringing copyright.
- Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords).
- Creating or propagating computer viruses or other harmful files.
- Unfair usage (downloading/uploading large files that hinders others in their use of the internet).
- Online gaming (educational).
- Online gaming (non-educational).
- Online gambling.
- Online shopping/commerce.
- File sharing.
- Use of social media.
- Use of messaging apps.
- Unsupervised use of video broadcasting e.g. Youtube.

Responding to incidents of misuse
This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities. (See attached Actions/Sanctions table).

Illegal incidents

If there is any suspicion that the website(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.

Online Safety Incident

Unsuitable Materials
→ Report to the person responsible for Online Safety
→ If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
→ Debrief on online safety incident
→ Review policies and share experience and practice as required
→ Implement changes
→ Monitor situation

→ Record details in incident log
→ Provide collated incident report logs to LSCB and/or other relevant authority as appropriate

Illegal materials or activities found or suspected

- Illegal Activity or Content (No immediate risk) → Report to CEOP
- Illegal Activity or Content (Child at Immediate Risk) → Report to Child Protection team
- Staff/Volunteer or other adult → Report to Child Protection team → Call professional strategy meeting

→ Secure and preserve evidence
→ Await CEOP or Police response

- If no illegal activity or material is confirmed then revert to internal procedures
- If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
  → In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other incidents

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

In the event of suspicion, all steps in this procedure should be followed:
- Have more than one senior member of staff/volunteer involved in this process? This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are

closely monitored and recorded (to provide further protection).

- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures.
    - Involvement by Bromley Safeguarding Board 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; or
    - other criminal conduct, activity or materials.
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school, and possibly the police, and demonstrate that visits to these sites were carried out for child protection 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. The Trust Code of Conduct and Staff Discipline Policy will be consulted when dealing with staff members who have engaged in inappropriate or illegal online behavior. Each incident will be dealt with on an individual basis where, in extreme cases, staff could face disciplinary proceedings or even dismissal.

Acknowledgements

Valley Primary School would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School E-Safety Policy:

- SWGfL E-Safety Group

Appendices

- Student/Pupil Acceptable Use Agreement template (KS1)
- Student/Pupil Acceptable Use Agreement template (KS2)
- Legislation
- Links to other organisations and documents

KS1 Computing Rules

S	**I will only use an iPad or computer with the permission of a trusted adult.**
A	**I will only use kind words online.**
F	I will only communicate online with people I know in real life, unless I have a trusted adult with me.
E	If I see something I don't like on a screen, I will always tell an adult.
T	I will always keep my passwords to myself.
Y	I will look after all IT equipment, including iPads and computers.

I have read these rules, and I will do my very best to follow them inside and outside of school.

My Name:

KS2 Pupil Acceptable Use Agreement

These rules will keep me safe and are part of the Valley Home-School Agreement. I understand that there may be consequences if I do not follow these rules <u>either at school, outside of school, and online.</u>

Conduct:
- I will only use the school's iPads/computers for educational use.
- I will only edit or delete my own files/online accounts and not change or log into other people's files/online accounts without their permission.
- I will keep my logins and passwords to myself.
- I will not bring files into school without permission or upload inappropriate material to my workspace.

Contact:
- The messages I send, or information I upload, will always be polite and sensible.
- I will only message people I know, or a responsible adult has approved.
- I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family, my school or my friends, unless a trusted adult has given permission.

Content:
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult, and try to take a screenshot as evidence.
- I am aware that some websites and social networks have age restrictions and I should respect this, as well as understand that these restrictions are in place to protect me.
- I will not attempt to visit Internet sites that I know to be banned by the school, or that would be inappropriate for home use.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.

*I have read and understand these rules and agree to follow them **at all times**, and be a good Digital Citizen.*

Signed (pupil):   *Date:*

Signed (parent):   *Date:*

Legislation
Below is 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.

General Data Protection Regulations (GDPR) 2018

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.
(http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screenin

g-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)

Links to other organisations or documents
Safer Internet Centre – http://saferinternet.org.uk/
South West Grid for Learning - http://swgfl.org.uk/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Internet Watch Foundation - https://www.iwf.org.uk/
CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm
UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
Netsmartz - http://www.netsmartz.org/

Tools for Schools
Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

Bullying / Cyberbullying
Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - http://enable.eun.org/
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet –Cyberbullying guidance and toolkit http://www.childnet.com/new-for-schools/cyberbullying-events/childnets-upcoming-cyberbullying-work
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Social Networking
Digizen – Social Networking
UKSIC - Safety Features on Social Networks
SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people
Connectsafely Parents Guide to Facebook
Facebook Guide for Educators

Curriculum
SWGfL Digital Literacy & Citizenship curriculum
Glow - http://www.educationscotland.gov.uk/usingglowandict/
Teach Today – www.teachtoday.eu/
Insafe - Education Resources

Mobile Devices / BYOD
Cloudlearn Report Effective practice for schools moving to end locking and blocking
NEN   - Guidance Note - BYOD

Data Protection
Information Commissioners Office:
Your rights to your information – Resources for Schools - ICO
Guide to Data Protection Act - Information Commissioners Office
Guide to the Freedom of Information Act - Information Commissioners Office
ICO guidance on the Freedom of Information Model Publication Scheme

ICO Freedom of Information Model Publication Scheme Template for schools (England)
ICO - Guidance we gave to schools - September 2012 (England)
ICO Guidance on Bring Your Own Device
ICO Guidance on Cloud Hosted Services
Information Commissioners Office good practice note on taking photos in schools
ICO Guidance Data Protection Practical Guide to IT Security
ICO – Think Privacy Toolkit
ICO – Personal Information Online – Code of Practice
ICO Subject Access Code of Practice
ICO – Guidance on Data Security Breach Management
SWGfL -   Guidance for Schools on Cloud Hosted Services
LGfL - Data Handling Compliance Check List
Somerset - Flowchart on Storage of Personal Data
NEN - Guidance Note - Protecting School Data

Professional Standards / Staff Training
DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs
Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support
Somerset - Questions for Technical Support
NEN - Guidance Note - esecurity

Working with parents and carers
SWGfL Digital Literacy & Citizenship curriculum
Online Safety BOOST Presentations - parent's presentation
Connectsafely Parents Guide to Facebook
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops / education
The Digital Universe of Your Children - animated videos for parents (Insafe)
Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
Insafe - A guide for parents - education and the new media
The Cybersmile Foundation (cyberbullying) - advice for parents

Research
EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011
Futurelab - "Digital participation - its not chalk and talk any more!"
Ofcom – Children & Parents – media use and attitudes report - 2015