SHERDLEY PRIMARY SCHOOL

E-safety Policy

Date Agreed by Governors: ____________________

Review Date: ___________________

Signed: _________________________ (Chair of Governors)

Signed: _________________________ (Headteacher)

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by a working group made up of:

- *Headteacher*
- *Computing Co-ordinators*
- *Staff – including Teachers, Support Staff, Technical staff*
- *Governors*

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the *Governing Body on:*	
The implementation of this e-safety policy will be monitored by the:	*SLT and ICT co-ordinators*
Monitoring will take place at regular intervals:	*Annually*
The *Governing Body* will receive a report on the implementation of the e-safety policy (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. The next anticipated review date will be:	
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*Agilisys, Police, Social Care, LADO*

The school will monitor the impact of the policy using:

- ○ *Any appropriately shared logs of reported incidents especially cpoms.*
- ○ *Our school website*
- ○ *Surveys / questionnaires of*
  - ▪ *students / pupils*
  - ▪ *parents / carers*
  - ▪ *staff*

Scope of the Policy

This policy applies to all members of the school (including staff, students / pupils, the before and after school club staff, 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 (see appendix for policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy and Anti-Bullying Policy.

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

It is accepted that although all reasonable measures will be taken, it is likely that there will be unforeseen circumstances and possible occasions of 'unsafe' behaviours or situations, despite ALL of the policy requirements being adhered to; such is the ever-changing nature of the electronic age.

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. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports via Governing Body meeting feedback at least bi-annually, but more often if incidents occur. A member of the Governing Body has taken on the role of E-Safety Link Governor, whose role incudes:

- meetings with the E-Safety Co-ordinator – Mr Peter Massey
- regular monitoring of e-safety incident logs as made available when appropriate by our Managed Service Provider

Headteacher and Senior Leaders:

- The Headteacher*, Mr T McCoy,* has a duty of care for ensuring the safety (including e-safety) of members of the school community
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. Mrs Robertson, the Deputy Headteacher is the other designated member of SLT who is aware of procedures to be followed in the event of a serious e-safety allegation being made.
- The Headteacher and Senior Leaders are responsible for ensuring that the E-Safety Coordinator 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 Headteacher 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.

E-Safety Coordinator:

The E-Safety Coordinator is Mr Peter Massey

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents alongside the Headteacher.
- 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, all volunteers and parents
- liaises with the Local Authority / relevant body
- liaises with school technical staff and Managed Service Providers
- is the designated contact for the Managed Service Provider to provide reports of e-safety incidents when appropriate, and creates a log of incidents to inform future e-safety developments,
- attends relevant meeting, i.e. school cluster meetings
- reports to Senior Leadership Team as appropriate.

Network Manager / Technical staff:

The Co-ordinator for ICT / Computing is responsible for ensuring that the school's technical infrastructure is, as far as possible, secure and is not open to misuse or malicious attack by checking that the Managed Network Provider :

- ensures, as far as possible, that the school meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.
- ensures, as far as possible, 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, and that breaches of this may occur despite all safe intentions and measures being carried out
- keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher

Teaching and Support Staff:

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the Sherdley e-safety policy and practices and will agree to adhere to them
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher 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 termly
- students / pupils understand and follow the e-safety and acceptable use policies within school
- students / 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

Child Protection / Safeguarding Designated Lead:

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
- cyber-bullying
- awareness of radicalisation or extremism via the internet.

Pupils:

- are responsible for following the Sherdley Computing Rules – agreement to be implemented in 2019-20
- 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 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, including the use of the 'Report' button on the VLE element of the school website

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. Sherdley 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 / blog
- their children's personal devices in the school (where this is allowed)

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, and to know what is appropriate should they encounter any 'unsafe' behaviour online.

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

- A planned e-safety curriculum is provided is part of Computing / PHCSE / other lessons and should be regularly revisited at least half termly
- Key e-safety messages are reinforced as part of a planned programme of assemblies and pastoral activities, including themed weeks and joining National awareness campaigns
- Pupils will 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 will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils will be helped to understand the need for the pupil Sherdley Computing Rules agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff will act as good role models in their use of digital technologies, the internet and mobile devices
- I n 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, and if inappropriate content is found, that pupils know the correct procedure.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit (by periodically scanning browser histories, walking around the room etc.), and pupils should be taught relevant measures to take if inappropriate material breaks through filters (informing a member of staff, and for older pupils, how to minimise the screen so that others do not see the offensive material.

- It is accepted that from time to time, for good educational reasons, pupils 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 (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents / carers

Many parents and carers have only a limited understanding of 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 evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications
- Delivering or facilitating the delivery of training/awareness sessions for parents and carers

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's 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 and local authority websites will provide e-safety information for the wider community
- Support will be given, if requested, to enable any community groups who work with pupils and parents of our school, to ensure that they are aware of best practices linked to E-Safety

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 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 annually. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All staff should receive annual e-safety training/updates as part of CPD programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events (e.g. from 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 Coordinator / Officer (or other nominated person) 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 / group 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
- Participation in school training / information sessions for staff where and when appropriate

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 ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities. Despite ALL measures being implemented it is accepted that breaches of filtering and 'safety' are likely to occur, in keeping with the constantly changing electronic world:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements, utilising the skills of a Managed Service Provider
- There will be regular reviews and audits of the safety and security of school academy technical systems
- Servers, wireless systems and cabling will be, as far as possible, securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- The Headteacher, Computing Coordinators and Managed Service Provider consultants are responsible for ensuring that software license logs are as accurate and up to date as possible, and that the number of licenses purchased against the number of software installations matches
- Internet access is filtered for all users. School technical staff regularly monitor and record the activity of users on the school technical systems and may report appropriate breaches to the Headteacher for further investigation
- 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.
- Guests and temporary staff must login using their own account, or at the very least utilise the login details of a member of staff who is continually present with that member of staff and the computer, and who has not shared their login details
- Personal data cannot be taken off site on any mobile device (including the hard drive of laptops). To access and work on personal data, staff must use the remote access to the school server (currently Junos). Data carried on mobile devices must not contain any personal data of any member of the school community.

  Breaches of personal data security are recognised as two categories; a purposeful breach is when data has been knowingly shared against confidentiality and e-safety policies with a purpose of intent. Non-purposeful breaches are seen as unintentional, one-offs, however repeated Non-purposeful breaches will be treated as 'Purposeful' through neglect or malpractice.

  The use of school iPads off site is permitted however all measures must be put into place to safeguard against the contents from the iPad being shared inappropriately. The iPad has a 4 digit lock code that must be enabled when off-site and then disabled when back at school. The iPads must be kept in a locked secure location when left unattended. The iPad must never be used on an unsecure 'open' Wi-Fi network.

  You should not take iPads off-site for personal use.

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 in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff 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, and cameras/storage discs should be wiped regularly to ensure that as little amount of exposed data is available should they be lost or stolen
- 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.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the GDPR 2018, 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 must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- 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 and current GDPR practices.

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, and that they lock the screen of any computer they are logged into when they are away from the screen.
- Transfer data using encryption and secure password protected devices.
- Maintain any equipment they have responsibility for as part of their role – making sure equipment is clean, stored and carried appropriately, not kept in cars overnight, ensure food and drinks are kept away from hardware.
- Do not share passwords with ANYONE, including if requested by Managed Service Provider or Headteacher – they should login themselves if requested to allow access.
- Follow the agreed protocol for reporting loss of any hardware in line with current GDPR practices.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

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 students / pupils or parents / carers (email) 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.
- The school Facebook page is overseen and managed by Mrs Carol Robertson – with appropriate profanity filters and security settings regularly updated. Anyone wishing to join the site is vetted and if appropriate denied access to the page.
- The school Twitter account is overseen and managed by Mr Tony McCoy.

- Pupils will be taught about e-safety issues, such as the risks attached to the sharing of personal details. They will also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- All iPads are connected to the same account and – whilst on site – do not need any passcode to use them. Therefore, the responsibility for their use will fall to the member of staff that is supervising the children using them. The class set is numbered and it will be sufficient to make a note on the children that are using a particular iPad for each session. Any issues with an iPad can then be traced back to a particular child or class using it.

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render Sherdley Primary School or the 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 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 which could have negative implications or lead to inappropriate comments
- 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 name is not brought into disrepute

The school Facebook page is managed and overseen by Mrs. Carol Robertson. All appropriate security settings are regularly updated, individuals who request access to the page are vetted and if appropriate denied access. The page contains no photographs or videos linked to the school staff or pupils and is purely intended as a vehicle for information sharing. Private messages sent via the page are dealt with by Mrs. Carol Robertson, sometimes in collaboration with the Headteacher as appropriate, and a clear trail of response if visible, including notification when a request for information has been denied or an alternative method of discussion arranged.

Our school Twitter account is overseen by Mr. Tony McCoy with any inappropriate content removed.