# Heron Way Primary School Online/Digital Policy

| Date | Review Date | Coordinator | Nominated Governor |
|---|---|---|---|
| Feb 2020 | **Feb 2023** | **Lena Cann/James Crump** | **Safeguarding Governor** |

# Heron Way Primary School Online/Digital Safety Policy

# Scope of the Policy

This policy applies to all members of the school community (including staff, 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 / 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.

# 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' resources Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding Governor.

The role of the Safeguarding Governor will include:

- regular updates from the ICT Leader
- monitoring of e-safety incident logs (stored on staff shared)
- reporting to relevant Governors during meeting

## Headteacher / Senior Leaders:

- The Headteacher 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 Computing Leader.
- 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 (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR disciplinary procedures).
- The Headteacher/Senior Leaders are responsible for ensuring that all other staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher/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 those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Computing Subject Leader.

## Computing Leader:

- leads e-safety in the school, working closely with the PSHCE leader.
- 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 the Local Authority, following consultation with the Headteacher.
- liaises with school technical staff.
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- provides updates to the Safeguarding Governor and shares current issues, reviews incident logs and filtering / change control logs.
- reports regularly to the Senior Leadership Team.

## ICT Technician:

The IT Technician 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 e-safety technical requirements and any Local Authority E-Safety 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 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/the VLE/remote access /email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Senior Leader/Computing Leader for investigation /action.
- that monitoring software/systems are implemented and updated as agreed in school policies.
- for supporting pupils and staff in using the internet responsibly and implementing the school's curriculum.
- a budget is supplied by the school for expert IT technicians to offer advice and practical support on all of the points above.

## Teaching and Support Staff:

All staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current Heron Way Primary School e-safety policy and practices.
- they have read, understood and signed the Staff Acceptable Use Policy/Agreement (AUP) – completed at staff induction.
- they report any suspected misuse or problem to the Headteacher/Senior Leader/Computing Leader for investigation/action.
- 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 class charter and acceptable use policies.
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- staff monitor the use of digital technologies, mobile devices (iPads, laptops) 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:

The Designated Safeguarding 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 material
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

## Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy.
- 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, within our virtual learning platform as well as beyond the school's learning platform.
- 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.

## 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, home-school diaries, the school's website, www.heronway.w-sussex.sch.uk or the school's learning platform. 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 school's website and learning platform.
- their children's personal devices in the school

## Community Users:

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

Guest access to the school's wireless network is provided through a single use key. The wireless network will be managed to ensure that guest devices are separated from internal computers and devices. All guest internet use is filtered and monitored.

# 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 and PSHCE lessons and should be regularly revisited.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and class 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 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. It is expected that children in Reception and KS1 would normally use websites carefully selected by the class teacher to ensure that content is relevant and age appropriate.
- 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, pupils may need to research topics (eg 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 specific sites from the filtered list for the period of study. **Any request to do so, must be requested in writing via email, with clear reasons for the need. The Head Teacher should approve these requests.**

## Education – parents/carers:

Many parents and carers may 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:

- Newsletters
- The E-Safety section on the school's website
- The school's learning platform
- Parent forum evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications eg www.saferinternet.org.uk/ http://www.childnet.com/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 website will provide e-safety information for the wider community
- Supporting community groups e.g. Early Years Settings, childminders, youth / sports / voluntary groups, to enhance their e-safety provision
- Within the HELP locality of local authority

# 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, which 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 be provided with access to this policy on induction, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The Computing Leader (or other nominated person) will receive regular updates through attendance at external training events (e.g. from 360 degrees / CAS / 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.
- The Computing Leader (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 (e.g. e-PD).
- 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 has a managed ICT service provided by an outside contractor, but it is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of Heron Way Primary School's E-Safety Policy / Acceptable Use Agreements. The school should also check their Local Authority / other relevant body policies on these technical issues.

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.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling will be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2 and above) will be provided with a username and secure password by the ICT 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 ICT system, used by the ICT Technician (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).

- The ICT 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. Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs.

Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.

- The school has provided enhanced / differentiated user-level filtering allowing different filtering levels for groups of users – staff / pupils.
- School technical staff regularly monitor and record the activity of users using and contributions to the school's learning platform.
- An appropriate system is in place for users to report any inappropriate use or concerns to the relevant person whilst using the school's hardware, mobile technology or the use of the internet including the school's learning platform.
- 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. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems – the provision here is that the 'guest' staff will be provided with a temporary network user name which will allow the guest to access the internet and shared network folders. The 'guest' users have to sign in and out any hardware which is used to support teaching and learning.
- An agreed policy is in place regarding the use of removable media (eg 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.

# 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. **Personal mobile devices should not be used for taking photographs.**
- 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. Consent will always be sought from parents before publishing photos.
- 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 to be covered as part of the agreement signed by parents or carers on entry to the school.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

# 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. 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 (e-mail, WhatsApp, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems such as the Virtual Learning Environment. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils may be provided with individual school email addresses for educational use. Email accounts are restricted and users can only send or receive emails to other Heron Way users.
- Email access is turned off by default for all pupils. Class teachers can request that these accounts are enabled to support teaching where it is relevant. Any communications will be monitored closely by staff.
- 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

With an increase in use of all types of social media for professional and personal purposes, a policy that sets out 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 e-safety framework 2012 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, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies 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, to include acceptable use, social media risks, checking of settings, data protection and 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

- staff do not engage in online discussion on personal matters relating to members of the school community
- personal opinions are not 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.

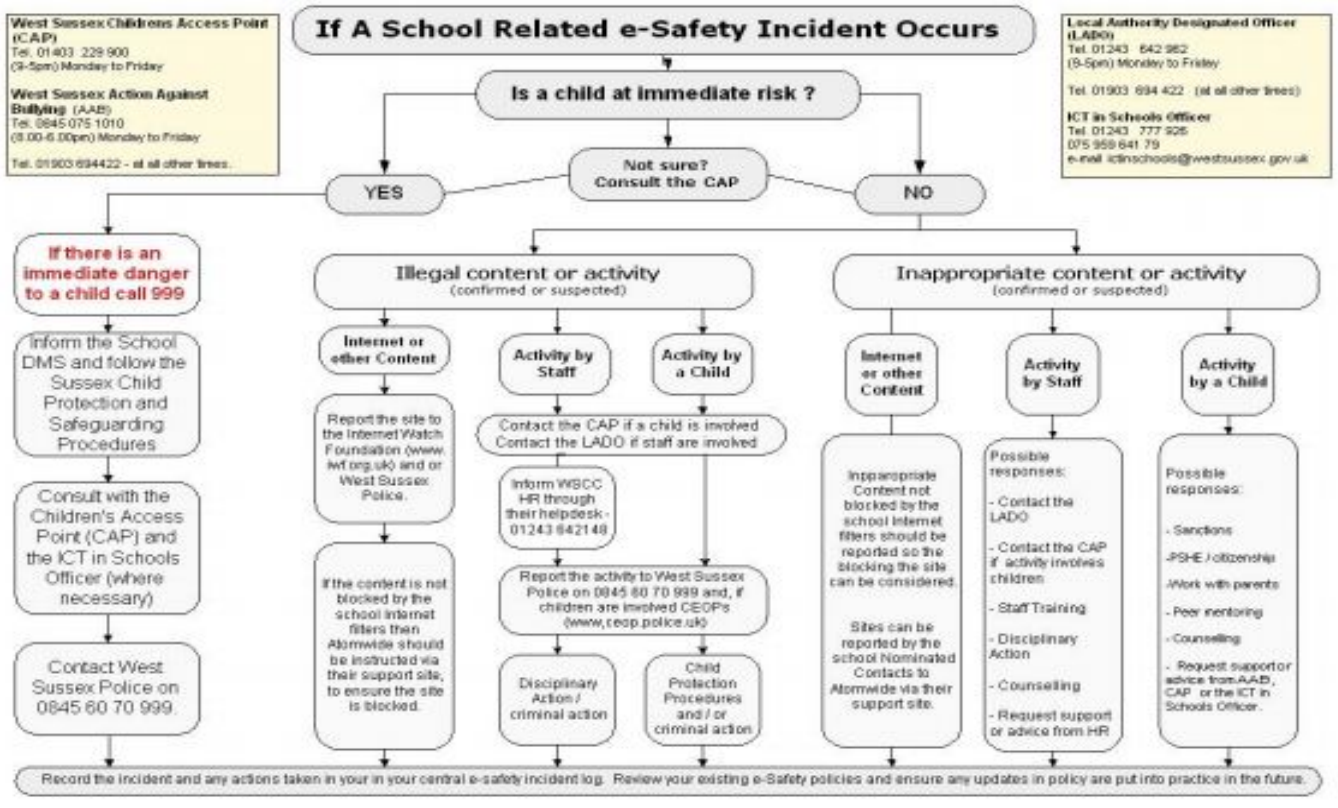
All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and / or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

# 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 and the appropriate action must be taken and recorded.

## 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, who understand and follow school policy, will be responsible users of digital technologies. However, there may be times when infringements of the policy could take place, through careless, irresponsible or 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 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
  - 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.

# Responding to incidents of misuse

**Record of reviewing devices / internet sites (responding to incidents of misuse)**

| | |
|---|---|
| Group | |
| Date | |
| Reason for investigation | |

**Details of first reviewing person**

| | |
|---|---|
| Name | |
| Position | |
| Signature | |

**Details of second reviewing person**

| | |
|---|---|
| Name | |
| Position | |
| Signature | |

**Name and location of computer used for review (for web sites)**

| |
|---|
| |

| **Web site(s) address / device** | **Reason for concern** |
|---|---|
| | |
| | |
| | |
| | |
| | |

**Conclusion and Action proposed or taken**

| | |
|---|---|
| | |
| | |
| | |
| | |
| | |

Reporting Log

| Reporting Log | | | | | | |
|---|---|---|---|---|---|---|
| Date | Time | Incident | Action taken | | Incident Reported by | Signature |
| | | | What? | By whom? | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

Reporting Log

# Development/Monitoring/Review of this Policy

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

- Senior Leaders
- Computing Leader
- 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.

## Monitoring and Review

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 pupils, parents / carers and staff