WINCHCOMBE SCHOOL	
E-Safety Policy	
Effective Date: May 2018 **Review Date: June 2018, September 2019** **Review Period: September 2021**	**Review Committee: Resources/PG/E-Safety Officer** **Leadership Team role responsible for the operation of the policy: Headteacher**

This Policy was reviewed and adopted by the Full Governing Body

Adopted		
Signature		**Headteacher**
Signature		**Chair of Resources**
Date		

E-Safety Policy

Contents:

1.1 E-Safety coordinator

Our E–Safety Policy has been written by the school and agreed by the Senior Leadership Team. The School has also appointed a member of the Governing Body to take lead responsibility for E-Safety

The School E-Safety Coordinator in school is Jay Buttler (Network Manager), the role is supported by a member of SLT, Parin Gohil, Deputy Headteacher (SENDCO & Behaviour).

1.2 Teaching and learning

1.2.1 Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Internet use is part of the statutory curriculum and is a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

1.2.2 How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- access to learning wherever and whenever convenient.

1.2.3 How can Internet use enhance learning?

- Pupils will be taught what Internet use is acceptable; what is not and given clear objectives for Internet use.
- The school will ensure that the copying and subsequent use of Internet-derived materials, by staff and pupils, complies with copyright law.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of: knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

1.2.4 How will pupils learn how to evaluate Internet content?

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

1.3 Managing Information Systems

1.3.1 Security

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured.
- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Portable media may not be used without specific permission, followed by an anti-virus / malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The network manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

1.3.2 E mail

- Staff will only use official school provided email accounts to communicate with pupils, parents/carers and professionals, as approved by the Senior Leadership Team.
- Access, in school, to external personal email accounts may be blocked.
- Emails sent to external organisations should be written carefully, in the same way as a letter written on school headed paper would be.
- Staff should not use personal email accounts during school hours or for professional purposes.

1.3.3 Management of published content

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published *(see Data Protection Policy)*
- Content published must be accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

1.3.4 Publishing of pupils' images or work

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs unless consent has been given from parents or carers.
- Written or electronic permission, from parents or carers, will be obtained before images/videos of pupils are electronically published.
- Pupils' work can only be published with their permission and the parents.
- Written or electronic consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.

1.3.5 Social networking, social media and personal publishing

- The school will control access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include: real name, address, mobile or landline phone numbers, school attended, IM and email addresses, user names/IDs, full names of friends/family, specific interests and clubs etc.
- Staff wishing to use Social Media tools with students, as part of the curriculum, will risk-assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain consent from the Senior Leadership Team before using Social Media tools in the classroom.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use, on a personal basis.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encouraged to approve and invite known friends, only, on social networking sites and to deny access to others by making profiles private.

- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful, defamatory or sexual.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

1.3.6 Filtering

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with its broadband provider/network manager to ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School E-Safety Coordinator or network manager, who will then record the incident and escalate the concern to SLT as appropriate.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- Any material that the school believes is illegal will be reported to appropriate agencies.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

1.3.7 Emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use or Mobile Phone Policy.

1.3.8 Protection of personal data *(see Data Protection Policy - GDPR)*

- The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union.

The GDPR sets out seven key principles:

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality (security)
- Accountability.

1.4 <u>Policy Decisions</u>

1.4.1 Authorisation of internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff will read and sign the School Acceptable Use Policy before using any school ICT resources.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- All visitors to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy.
- Parents will be informed that pupils will be provided with supervised internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).
- Students will apply for Internet access individually by agreeing to comply with the School E–Safety Rules or Acceptable Use Policy.

1.4.2 Assessing the risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use, to establish if the E–Safety policy is adequate and that the implementation of the E–Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported.
- Methods to identify, assess and minimise risks will be reviewed regularly.

1.4.3 Causes for concern

- All members of the school community will be informed about the procedure for reporting E-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The Designated Safeguarding Lead will be informed of any E-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage E-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team.

1.4.4 Handling E–Safety complaints

- Complaints about internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the Head teacher.
- All E–Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

1.4.5 Internet use and the local community?

- The school will liaise with local organisations to establish a common approach to E–Safety.
- The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.

1.4.6 Cyberbullying

- Cyberbullying (along with all other forms of bullying), of any member of the school community, will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- There are clear procedures in place to investigate incidents of cyberbullying and to support anyone in the school community affected by cyberbullying. *(See Behaviour Policy)*
- All incidents of cyberbullying reported to the school will be recorded.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's E-Safety ethos.
- Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

1.4.7 Office 365 & One Drive (Shared Access)

- SLT and staff will regularly monitor the usage of the Office 365 and One Drive by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the Office 365 and One Drive.
- Only members of the current pupil, parent/carers and staff community will have access to Office 365 and One Drive.
- All users will be mindful of copyright issues and will only upload appropriate content onto Office 365 and One Drive.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Any concerns about content on Office 365 and One Drive may be recorded and dealt with in the following ways:
  a) The user will be asked to remove any material deemed to be inappropriate or offensive.
  b) The material will be removed by the site administrator if the user does not comply.
  c) Access to Office 365 and One Drive for the user may be suspended.
  d) The user will need to discuss the issues with a member of SLT before reinstatement.
  e) A pupil's parent/carer may be informed.
- A visitor may be invited onto Office 365 and One Drive by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

1.4.8 Mobile phones and other personal devices

- The use of mobile phones and other personal devices, by students and staff in school, will be decided by the school and covered in the School Acceptable Use or Mobile Phone Policies.
- The sending of abusive, or inappropriate, messages or content, via mobile phones or personal devices, is forbidden by any member of the school community: any breaches will be dealt with as part of the school discipline/behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be taken by the Senior Leadership Team. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times and placed in the school bag or locker.
- Electronic devices of all kinds, that are brought into school, are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within, or outside of, the setting in a professional capacity. Staff will be issued with a school phone where contact with pupils or parents/carers is required.
- If members of staff have an educational reason to allow children to use mobile phones or personal device, as part of an educational activity, then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.

1.5 Communication

1.5.1 E-Safety for students

- All users will be informed that network and internet use will be monitored.
- An E–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- Pupil instruction, regarding responsible and safe use, will precede internet access.
- An E–Safety module will be included in the PSHE/Tutorial programme, covering both safe school and home use.
- E-Safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to E-Safety education will be given where pupils are considered to be vulnerable.

1.5.2 Involving staff

- The E–Safety Policy will be formally provided to, and discussed with, all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff will be made aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible internet use, both professionally and personally, will be provided for all members of staff.
- Staff who manage filtering systems, or monitor ICT use, will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

1.5.3 Parental support

- Parents' attention will be drawn to the school E–Safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to E-Safety at home and at school, with parents, will be encouraged. This may include offering Parents' Evenings with demonstrations and suggestions for safe home internet use, or highlighting E–Safety at other attended events.