Longdean School

E-safeguarding Policy

Reviewed: **Autumn 2018**

Ratified: **December 2018**

Next Review **Autumn 2019**

1. Introduction

This policy encompasses Digital Technologies including the Internet and Electronic Communications including the use of Mobile Devices such as Phones, iPods, Kindles, Smart Watches, Tablets, and other wireless technology. It highlights the need to educate children and young people about the benefits and risks of using existing and emerging technologies and provides safeguards and awareness for users to enable them to control their online experiences. The policy aims to ensure that the internet and devices are used effectively for their intended purpose, without infringing legal requirements or creating unnecessary risk to raise standards and achievement whilst ensuring the safeguarding of all stakeholders.

The Longdean E-safeguarding Policy has been agreed by the senior management and approved by Trustees. It will be reviewed annually in accordance with the policy review schedule taking into account any changes in IT infrastructure and government guide lines.

2. Why use of Digital Technologies including the Internet is important

- The purpose of Digital Technology and 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 information and business administration systems, and is a ubiquitous tool for all stakeholders. It's use is an entitlement where a responsible use is adhered to

- The prime purposes of Longdean school's Website is to promote the school and to provide a learning environment from the school site or home, as well as to enable access of Staff, Students, Parents, Community and Business to the site

3. How Digital Technologies benefit education

Benefits of using the Internet in education include:

- Access to world-wide educational resources and learning environments and materials, museums, art galleries, educational and cultural exchanges between students, mentoring and support, remote access to files in school from beyond the school, access to experts and to report any e-safeguarding incidents

- Staff professional development through access to national developments, educational materials and good curriculum practice, communication with support services, professional associations and colleagues, exchange of data with the LEA, DfES and partner institutions

4. Learning with Digital Technologies

- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use

- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of students

- Staff should guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity

5. How Students will learn to evaluate Digital Content and safeguard stakeholders:

- When staff or students discover unsuitable sites, the URL (address) and content must be reported to the ICT Support team or Assistant Headteacher overseeing the network.

- Ensure that the use of Internet derived materials by staff and by students complies with copyright law

- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work. No attempt should be made to pass off Internet material as their own work. Students are made aware of the JCQ regulations regarding plagiarism and paraphrasing in their ICT / Computing lessons

- Training is available to staff in the evaluation of Web materials and methods of developing students' critical attitudes and how to keep all stakeholders safe online

6. Management of communications

- Students are directed to only use approved online systems

- Students must immediately tell a teacher if they receive offensive communications

- Students must not reveal details of themselves or others in communications, such as address or telephone number, inappropriate images, video or text, or arrange to meet anyone

- E-mail sent to an external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper

- The forwarding of chain or junk communications is not permitted

- Staff should only use the school e-mail address and not personal ones when acting on behalf of the school

- Users must not create access or share inappropriate content, including, but not limited to content containing the following items. Any such use must be reported immediately to the ICT Support, Pastoral, or Senior Leadership team

- Indecent images of children, discrimination of any kind, Promoting racial or religious hatred, Promoting illegal acts, or any other content which may be offensive to stakeholders, such as abusive images; promotion of violence; gambling; criminally racist or religious hatred material detrimental to Longdean

- Students must adhere to the rules around the use of mobile devices in school as laid out in the positive behaviour and section 9 of this policy.

- If you feel that your child should be exempt from this policy due to special educational needs, medical or disability, please write to the headteacher detailing your reasons for this consideration. All cases will be reviewed on an individual basis. To reach an informed decision you may be requested to provide evidence from a professional to demonstrate that a mobile device is required to alleviate the reasons identified in your letter.

School Consent Form

For students above the age of 16 and not living at home or for students 18 or older, the school should be able to rely on the consent of the pupil alone. Otherwise parent's consent must be obtained.

	Longdean School **Responsible ICT and Internet Use** **Please read, complete, sign and return to the school office**	
Student:	***Form:***	

Student's Agreement

I have read and I understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey the rules at all times.

I understand that all use of the connection is monitored and logged, and any misuse, such as, but not restricted to, downloading music, videos, software unrelated to school work, any unethical, immoral or illegal use, such as pornographic, racist, sexist, violent or otherwise offensive content, and that repeated access to, or a failure to report, unsuitable material once found, will result in the termination of the connection and disciplinary action which could result in exclusion from the school and appropriate legal action being taken including that required by the PREVENT duty.

I will not hold the school responsible for any materials acquired by, or communicated through this connection, or any perceived damage to equipment through its use. Longdean School accepts no responsibility for student's own equipment.

I understand that any unsuitable material found will be reported, upon discovery, to the ICT support team, who will review the material and, if required, block further access to it. The decision of Longdean School in any dispute regarding suitability is final.

Signed:	***Date:***

Parent's Consent for Internet Access on school owned devices

As the parent or guardian of this student, I understand that the student is agreeing to access to an internet connection at school, that I approve of this use and give permission for my son / daughter to access the school ICT systems including the Internet.

I understand that all use of the connection is monitored and logged, and any misuse, such as, but not restricted to, downloading music, videos, software unrelated to school work, any unethical, immoral or illegal use, such as pornographic, racist, sexist, violent or otherwise offensive content, and that repeated access to, or a failure to report, unsuitable material once found, will result in the termination of the connection and disciplinary action which could result in exclusion from the school and appropriate action being taken including that required by the PREVENT duty.

I will not hold the school responsible for any materials acquired by, or communiqué through, or damages arising from the use of this connection however; I understand that the school will take all reasonable precautions to ensure students cannot access inappropriate materials.

I understand that any unsuitable material found will be reported, upon discovery, to the ICT support team, who will review the material and, if required, block further access to it. The decision of Longdean School in any dispute regarding suitability is final. I confirm that I have discussed appropriate use of communications technology including appropriate use of Social Media both inside and outside of school including the age restrictions imposed by Social Media services with my child.

Signed:	***Date:***

Parent's Consent for student use of personal devices and BYOD Access to the school Wi-Fi and internet connection

In addition to the above agreement for Internet Access on school owned devices, I agree that my son/daughter may access the school's filtered internet from their own device. I will not hold the school responsible for any materials acquired by, or communiqué through this connection, or any perceived damage to equipment through its use. I accept that Longdean School has no responsibility for the student's own equipment or any perceived damage to equipment through its use, and that the student will comply with the agreement above regardless of the internet connection or device.

Signed:	***Date:***

Parent's Consent for reuse of digital likeness

I agree that the school may use my son / daughter digital likeness for example video, audio, picture text or their work in any way compliant with the school's safeguarding policies, including publishing these online. This will not enable students to be clearly identified as individuals without additional parental consent.

☐ I agree for use by Longdean stakeholders including partner education institutions such as co-operative schools, colleges with compatible safeguarding rules.

☐ I agree for use by third party institutions that Longdean agree to share information with, such as linked sports groups, press television.

Signed:	***Date:***
Please print name:	

Longdean School E-Safety Policy Addendum – Emerging Technologies: Social Networking

Many Adults work in schools use the web and social networking services such as Facebook, Bebo, My Space, Flikr etc personal use. Whilst school employees are private individuals, and have the right to use such services to communicate and share with friends and relatives across the globe, they also have professional reputations and careers to maintain.

Staff are strongly advised, in their own interests, to take steps to ensure that their personal data is not accessible to anybody who does not have permission to access it. All staff need to be aware that parents and pupils may carry out web and social network service searches to find on-line information about staff - background, interests, career experiences and self-presentation. All staff, especially new staff, those in training and induction, are advised to ensure that information available publicly about them is accurate and appropriate.

Colleagues are advised to ensure that they enable all privacy and security settings on their social networking accounts, including the prevention of messages being sent to them as a result of an internet search. This will prevent young people accessing and potentially misusing their personal information, or making inappropriate contact.

Once information is posted on the internet it enters the public domain. Even if security is set on such sites that only 'friends' can see your activities, these friends can pass the information on to others, and re-post on the internet. This can lead to instances of identity theft and cyber bullying, and can seriously affect reputations and careers.

Adults working in Longdean are advised to deny access as 'friends' to students or parents of students. This includes alumni, such as students who have gone on to higher education. It is recognised that there will be rare occasions where students or parents are close personal friends or relatives of Adults working in Longdean. Colleagues are advised that to consider carefully these situations, compare appropriateness of electronic communications with those you would be comfortable putting on paper. If you are unsure, please seek advice from the Assistant Headteacher responsible for e-learning.

All school related e-communications should be made using official school methods – Exchange e-mail, Portal, SLG, or School Telephone / Mobile. Records of verbal communications should be maintained in case of future query. If it is necessary in an emergency to use a personal mobile or landline, then colleagues are encouraged to use 141 before dialling to protect their mobile or landline number.

Social Networking is an ideal medium for 'co-constructive' learning, for sharing ideas, working collaboratively, reflecting on work, and for constructively criticising work.

Facilities exist within our internet that mirror social networking sites, in a safe educational environment.

This is a non-exhaustive list:

Educational Use	Commercial Website
Personal / Public Reflection	Facebook, Twitter, My Space, Blogger
Showcase – Information	Facebook, My Space, Bebo
Showcase – Photos	Flikr, Picassa
Showcase – Video	YouTube, Facebook
Showcase – Audio	Soundpedia, My Space, Bebo
Open editing of documents	Wikipedia
Chat / Messaging	MSN, Live, YIM, Twitter, Facebook

All use of the internet is logged. Any e-safety issues can be followed up and fed through existing school pastoral system.

Within School, access to social networking sites is denied to pupils through the school network on the Herts Grid. Network activity is monitored using ISA and 'Ranger' software. Any attempts to circumvent these filters, including using anonymous proxies are checked and logged weekly. Any e-safety issues are fed into the existing pastoral system on a case by case basis. All computer use, including the use of the internet on both connections is logged.

Staff have access to social networking sites through the Opal/Open Reach internet connection. They should consider their use carefully during their own time, such as lunchtime or after school. All use of the Opal/Open Reach line is logged using ISA.

Students are advised on e-safety during lessons in Year 7, and are reminded throughout the school on the internet, during PSCHE lessons, and as it arises in the wider curriculum.

E-safety incidents inside school, and incidents related to school occurring outside of school, should be reported to the ICT support team for investigation, the results of which will be fed into the pastoral system, and on to external agencies as required.

E-safety incidents outside of school not related to school should be logged with ceop through the thinkuknow website below:

Advice for staff and young people regarding social networking sites is available here:

http://www.thinkuknow.co.uk/

7. Management of Web site content

- The point of contact on the Web site will be the school address, school e-mail and telephone number. Staff or students' home information will not be published

- Web site photographs that include students will be selected carefully and will not enable individual students to be clearly identified

- Students' full names will not be used on the Website in association with photographs

- Written permission from parents or carers is obtained before photographs of students are published on the school Web site as part of the Computer Use Agreement

- The Assistant Headteacher and web team take overall editorial responsibility to ensure that content is accurate and appropriate

- The Web site complies with the school's guidelines for publications

- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained

8. Newsgroups, e-mail lists, chat rooms and social media

- Newsgroups may be made available to students through the internet, but only when an educational requirement for their use has been demonstrated

- Students will be advised never to give out personal details of any kind which may identify them or their location

- Students will not be allowed access to public or unregulated chat rooms or social networks

- Students will only be directed to use regulated monitored educational social environments such as those provided by the learning platform, Microsoft Yammer or Google Classroom. This use will be supervised and the importance of safeguarding revisited during use.

9. Managing emerging technologies

- Mobile devices are not to be seen or heard or used on site between 08:15 and 15:30. Post16 students can use mobile devices in their study areas only in lesson time and study areas at break and lunchtimes.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed

- Staff use of phones – technology is permitted but staff should be mindful of their professional obligations and duties

- If a stakeholder of Longdean, staff, student, Trustee or parent, takes a video, audio, picture or text (Digital Likeness) of another stakeholder, under the direction of a stakeholder of staff, they should only use this digital likeness for the purposes directed by the staff stakeholder. It should not be retained by the stakeholder, uploaded to social media sites, storage beyond the school, such as cloud storage, or forwarded to people beyond the school. The digital likeness should be uploaded, the school network, or other safeguarded

school system, to then be worked with, and deleted from the original device. As the digital likeness was captured on behalf of the school, it remains the copyright of the school regardless of the device or stakeholder taking it. When that stakeholder is no longer associated with Longdean, such as leaves the school, they will remove the digital likeness and any hard or digital copy will remain in the school.

- Owing to the potential surreptitious nature of their use, we recommend in order to safeguard themselves and others, no stakeholder in Longdean should wear a Smart Watch in public areas of the school. Any use of a Smart Watch is subject to the same safeguarding rules as any personal device such as a mobile phone.

- Pupils agree not to sign up to online services until they are old enough to do so. In most cases this is from the age of 13.

- The school actively monitor students' usage for signs of online radicalisation as part of the Prevent Strategy, through classroom management software, internet logging and filtering. It recognises that staff vigilance plays an important role as students increasingly carry their own internet connections with them on their personal devices, and as such classroom management software, internet logging and filtering on the school network is only part of identifying and managing potential or actual radicalisation. Lessons and assemblies are delivered around awareness of radicalisation, the potential causes and consequences.

- Cyber bullying will not be tolerated, any evidence of this must be reported immediately and appropriate action taken in accordance with the school's anti-bullying and safeguarding policy

10. Authorisation of use of School ICT Systems, including Internet access

- The school keeps a record of all staff and students who are granted Internet access. This is held in ICT Support. The record is kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn

- Students must apply for ICT and Internet access individually by agreeing to abide by the Responsible Internet Use statement that appears on the desktop of the school's computers. They will fill out a consent form that is also signed by their parents/guardians

- 6th form students using their own laptops or tablets or smart phones in school will access the school internet via a unique wireless portal which will be monitored once they and their parents have signed a separate BYOD agreement

11. Risk Assessment

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access but will act to block any inappropriate material once reported

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990

- The Headteacher will ensure that the e-Safeguarding Policy is implemented and compliance with the policy monitored via the Leadership Team

12. Introduction of the policy to Students

- Rules for Internet access are posted on the desktop of all student computers. Students sign the ICT Use agreement which has an overview of the rules

- Students are informed that Computer and Internet use will be monitored by ICT/Computing teachers, as part of Year 7 introduction lessons

- Instruction in responsible and safe use precedes Internet access in the first Year 7 classes, as part of a module on responsible internet use. Messages repeating this are given to all years in e-safety assemblies annually and by ICT teachers throughout the curriculum including the PSHE curriculum and as it arises in the wider curriculum

13. Staff consultation

- All staff must accept the terms of the 'Responsible Computer and Internet Use' statement before using any Internet resource in school

- All staff including teachers, supply staff, classroom assistants and support staff, will be directed to the School Internet Policy, and its importance explained as part of their induction and revisited in on-going CPD and annually in Safer Internet Week

- Staff should be aware that Internet traffic is monitored and traced to the individual user. Discretion and professional conduct is essential

- The monitoring of Internet use is a sensitive matter. Staff who operates the monitoring procedures should do so under the direction and supervision of the Senior Leadership Team.

14. Management of the ICT system

- The school ICT systems will be reviewed regularly with regard to security and safeguarding

- The transport of data in and out of the school should be conducted using the encrypted remote connections available, such as Ranger Outpost. The use of portable storage, such as memory sticks of Optical Disks should be considered carefully as to their security and suitability

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998

- Unapproved system utilities and executable files will not be allowed in students' work areas or attached to e-mail for use in school

- All files held on the school network or school approved external systems are checked when required by ICT Support routinely, and specifically under the direction of the SLT. The school exercises its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound

15. Handling of Complaints regarding Computer, Internet or Mobile Technology use

- E-safeguarding incidents inside school, and incidents related to school occurring outside of school, should be reported to the ICT support team or pastoral team for investigation, the results of which will be fed into the pastoral system, and on to external agencies as required including the Police

- Responsibility for handling incidents is delegated to a member of the Senior Leadership Team and the ICT Support team. Allegations regarding Stakeholder misuse will be investigated, and where necessary referred to the Head teacher. The stakeholders are informed of the process of the investigation which will vary depending on the nature of the allegation

- Investigations will include pastoral support colleagues who handle incidents which feed into the other safeguarding and behavioural systems. Student sanctions will vary depending on the severity and nature of the incident

16. Enlisting support of Parents

- Parents' attention is drawn to the School Internet Policy in admission paperwork, newsletters, during Safer Internet Week and in parental e-safety sessions

- Internet and Communication issues will be handled sensitively to inform parents without undue alarm by the ICT and pastoral teams. A partnership approach to resolving issues is taken with parents, including those that may have begun outside of school but manifest themselves in school

- Parents agree that they will ensure that their online activity would not cause any stakeholder distress or bring the school community into disrepute. They agree that they will

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

- Parents agree to support the school's policy and help prevent their children from signing up to online services until the children are old enough to do so. In most cases this is from the age of 13, and agree to close any that are found in use by their underage children

- Parents agree to support the rules around the use of mobile devices in school

17. Social Networking

- Many Adults working in schools use the web and social networking services such as Facebook, Bebo, My Space, Flikr, twitter, snapchat, instagram etc personal use. Whilst school employees are private individuals, and have the right to use such services to communicate and share with friends and relatives across the globe, they also have professional reputations and careers to maintain

- Staff are strongly advised, in their own interests, to take steps to ensure that their personal data is not accessible to anybody who does not have permission to access it. All staff need to be aware that parents and pupils may carry out web and social network service searches to find on-line information about staff - background, interests, career experiences and self-presentation. All staff, especially new staff, those in training and induction, are advised to ensure that information available publicly about them is accurate and appropriate

- Colleagues are advised to ensure that they enable all privacy and security settings on their social networking accounts, including the prevention of messages being sent to them as a result of an internet search. This will prevent young people accessing and potentially misusing their personal information, or making inappropriate contact

- Once information is posted on the internet it enters the public domain. Even if security is set on such sites that only 'friends' can see your activities, these friends can pass the information on to others, and re-post on the internet. This can lead to instances of identity theft and cyber bullying, and can seriously affect reputations and careers

- Adults working in Longdean are advised to deny access as 'friends' to students or parents of students. This includes alumni, such as students who have gone on to higher education. It is recognised that there will be rare occasions where students or parents are close personal friends or relatives of Adults working in Longdean. Colleagues are advised that to consider carefully these situations, compare appropriateness of electronic communications with those you would be comfortable putting on paper. If you are unsure, please seek advice from the AHT responsible for e-learning

- All school related e-communications should be made using official school methods – Exchange e-mail, or School Telephone / Mobile. Records of verbal communications should be maintained in case of future query. If it is necessary in an emergency to use a personal mobile or landline, then colleagues are encouraged to use 141 before dialling to protect their mobile or landline number

- Social Networking is an ideal medium for 'co-constructive' learning, for sharing ideas, working collaboratively, reflecting on work, and for constructively criticising work.

- Facilities exist within our website that mirror social networking sites, in a safe educational

environment. Where they cannot be replicated effectively, the risk associate with an external provider should be assessed and where control over content cannot be assured, parental consent of using an existing system under the direction of the school should be sought

Educational Use	Commercial Website	
Personal / Public Reflection	Facebook, Twitter, My Space, Blogger	
Showcase – Information	Facebook, My Space, Bebo	Forum
Showcase – Photos	Flikr, Picassa Commercial Website	Lightbox
Showcase – Video	YouTube, Facebook	FlowPlayer
Showcase – Audio	Soundpedia, My Space, Bebo	Podcast
Open editing of documents	Wikipedia	Wiki
Chat / Messaging	MSN, Live, YIM, Twitter, Facebook	Messaging Service, Chat

This is a non-exhaustive list:

All use of the internet is logged. Any e-safety issues can be followed up and fed through existing school pastoral system.

Within School, access to social networking sites is denied to pupils through the school network on the Herts Grid. Network activity is monitored using ISA and 'Ranger' software. Any attempts to circumvent these filters, including using anonymous proxies are checked and logged weekly. Any e-safety issues are fed into the existing pastoral system on a case by case basis. All computer use, including the use of the internet on both connections is logged.

Staff have access to social networking sites through the Open Reach internet connection. They should consider their use carefully during their own time, such as lunchtime or after school. All use of the Open Reach line is logged using ISA.

Advice for staff and young people regarding social networking sites is made available in lessons, safer internet week as listed previously in the policy.

E-safety incidents outside of school not related to school should be logged with ceop through the thinkuknow website at http://www.thinkuknow.co.uk/