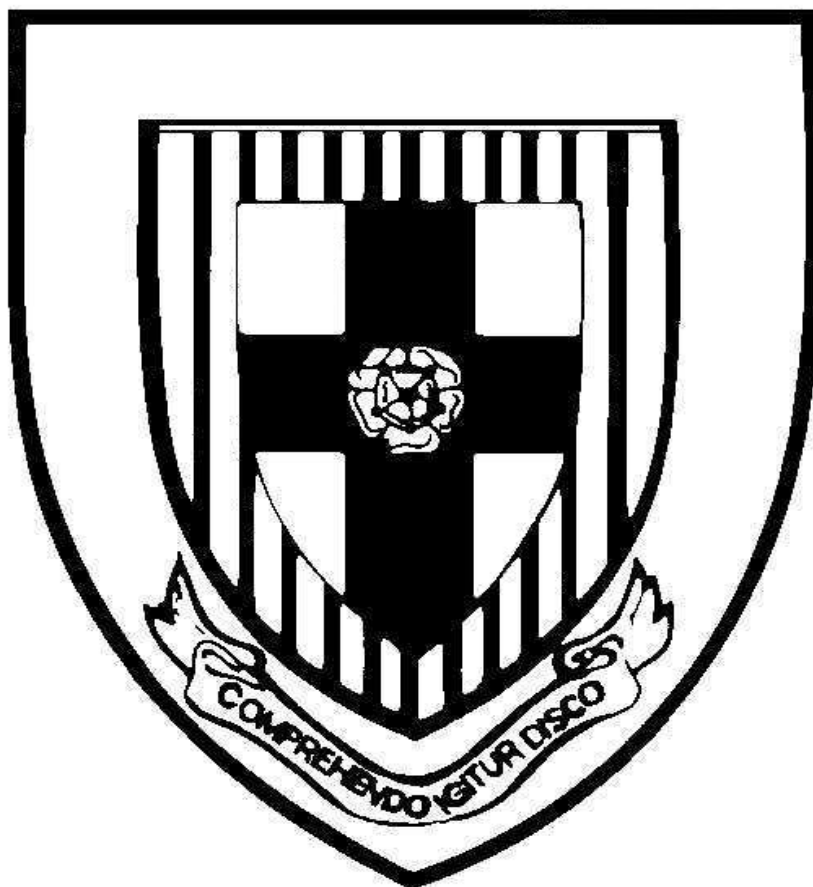




**E-SAFETY
POLICY**

November 2023

OAK COTTAGE E-SAFETY POLICY

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience and learn and work in a safe online environment.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- o **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- o **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- o **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- o **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

1) Roles and Responsibilities

The Headteacher and governors have ultimate responsibility to ensure that the e-safety Policy is monitored.

Our e-safety co-ordinator is: **Mr C Swain**

All members of the school community have been made aware of who holds this post. It is the role of the e-safety co-ordinator to keep abreast of current issues and guidance.

Senior Management and Governors are kept informed by the e-safety co-ordinator. All governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice. Governors will review the e-safety policy on an annual basis.

1.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the

designated safeguarding lead (DSL). The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is the safeguarding governor.

All governors will:

- o Ensure they have read and understand this policy
- o Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- o Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- o Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

1.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

1.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputy are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- o Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- o Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- o Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- o Working with the ICT manager to make sure the appropriate systems and processes are in place
- o Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- o Managing all online safety issues and incidents in line with the school's child protection policy

- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

1.4 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing
- Following the correct procedures by notifying a senior member of staff if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

1.5 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)
- Hot topics – [Childnet International](#)
- Parent resource sheet – [Childnet International](#)

1.6 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

The school's E-safety policy will operate in conjunction with other policies including those for Child Protection, Computing, Behaviour, Health and Safety, Curriculum, Mobile Device policy and Data Protection and Security.

2) Teaching and learning

Pupils Will be taught about online safety as part of the curriculum.

2.1) Why is Internet use important?

The internet is an essential element in 21st century life for education, business and social interaction. It is an open communications channel allowing information to be transmitted to many locations in the world. Messages may be sent, ideas discussed and material published, with very little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

The purpose of Internet use in school is to increase pupil achievement, to support the professional work of staff and to enhance the school's management, information and business administration systems. Benefits of using the internet in education include:

- Access to world-wide educational resources
- Inclusion in government initiatives such as the National Education Network (NEN) and teacher net (www.teachernet.gov.uk)
- Educational and cultural exchanges between pupils worldwide
- Cultural, vocational, social and leisure use in libraries, clubs and at home
- Access to experts in many fields for pupils and staff
- CPD through access to national developments, educational materials and good curriculum practice
- Communication with support services, professional associations and colleagues
- Improved access to technical support including remote management of networks
- Exchange of curriculum and administration data with the LA and DFE

The statutory curriculum requires pupils to learn how to create, organise, store, manipulate and retrieve digital content. In addition they need to identify where to go for help and support when they have concerns about content or contact on the internet. Also pupils need to search technologies effectively. Consequently, in delivering the computing curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail to enrich and extend learning activities.

2.2. Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and includes filtering content so that it is appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

2.3. Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- An E-Safety training programme will be delivered to all pupils to raise the awareness and importance of safe and responsible use of the Internet and other electronic communications tools. This is planned into the Computing curriculum for all year groups.

2.4. Engagement and education of children and young people to be considered vulnerable

- The school is aware that some children may be considered to be more vulnerable online due to a range of factors. Oak Cottage will ensure that differentiated and ability appropriate online safety education is given.

3) Core Principles of Internet Safety

In common with most technologies, Internet use presents risks as well as benefits. Pupils could be placed in inappropriate and even dangerous situations without mediated Internet access. To ensure responsible use and the safety of pupils the school's policy is built on the following five core principles:

Guided educational use

Internet use will be planned, task orientated and educational within a regulated and managed environment.

Risk assessment

Both staff and pupils will be aware of the risks associated with Internet use. Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school is allowed. Staff and pupils will know what to do if they come across inappropriate material when using the Internet.

Responsibility

Internet safety depends on staff, governors, advisors, parents, and, where appropriate, pupils themselves taking responsibility for use of the Internet and associated technologies. The school will seek to balance education for responsible use, regulation and technical solutions to ensure pupils' safety.

Regulation

The use of the Internet, which brings with it the possibility of misuse, will be regulated. Fair rules, written for pupils to read and understand, are prominently displayed as a constant reminder of the expectations regarding Internet use.

Appropriate Strategies

Effective, monitored strategies are in place to ensure responsible and safe Internet use. The school will work in partnership with the LA, DFE, parents and the Internet Service Provider to ensure systems to protect pupils are regularly reviewed and improved.

4) Managing Internet Access

4.1 Information system security

- School ICT systems capacity and security are reviewed regularly.
- Virus protection is updated regularly.
- Security strategies are discussed with Solihull LA.

4.2 E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone, without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised by the class teacher, before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

4.3 Published content and the school web site

- The contact details on the web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published, apart from names.
- The School Business Manager and Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

4.4 Publishing pupil's images and work

- Pupils' full names will not be used on the web site in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

4.5 Social networking and personal publishing.

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, email address, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils and parents should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name, school or shopping centre.
- Parents are informed that photographs or videos of any dress rehearsal or actual performance should only be used for their own domestic purposes and not published on social media.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others. They should be advised not to publish specific and detailed private thoughts.
- School staff should ensure that they do not communicate with pupils through private social networking sites even on educational matters, but should use official sites sanctioned by the school.

4.6 Managing Filtering

- The school will work in partnership with Solihull MBC to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to Solihull ICT Services and where appropriate the school e-Safety officer.

4.7 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.

4.8 Video Conferencing (including internet telephony such as skype)

- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer
- IP video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses should not be made available to other sites.
- Video conferencing contact information should not be put on the school website.
- Pupils should ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing should be supervised appropriately for the pupils' age.
- When recording a lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.
- Recorded material shall be stored securely.
- If third-party materials are to be included, check that recording is acceptable to avoid infringing the owners' Intellectual Property Rights (IPR).

4.9 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Oak Cottage Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. Oak Cottage Primary School will treat any use of AI to bully pupils in line with our Behaviour Policy.

Generative Artificial Intelligence represents many opportunities to support the development of lesson planning, teaching input and lesson resources. However, the content of the final document remains the professional responsibility of the person who produced it and the organisation they belong to. Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school and particularly if in connection with work undertaken by pupils.

2. Protecting staff and pupils is paramount and the use of AI must be monitored and supervised to ensure that data is not collected and used to train generative models.

4.10 Protecting personal data

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

4.11 Password Policy

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.
- From Nursery, all pupils are provided with their own unique username and private passwords to access school systems. Pupils are responsible for keeping their password private.
- We require staff and pupils to use STRONG passwords for access into our system.
- We require staff and pupils to change their passwords if they are compromised.

5) School rules

The school has developed a set of guidelines for Internet use by pupils. These rules will be made available to pupils and kept under constant review. All members of staff are responsible for explaining the rules and their implications. All members of staff need to be aware of possible misuses and their responsibilities towards pupils.

5.1 Pupils

The following rules apply to Foundation Key Stage and Key Stage One pupils:

- When sending an e-mail, I will not give any information about myself or my family.
- If I see anything I am unhappy with, or I receive messages I do not like, I will tell a teacher straight away.
- I can post sensible and kind messages about my lesson on Google Classroom (class stream and in the classwork section).
- I can only use the internet when I have asked an adult.
- I can click on the buttons or links when I know what they do.
- I will always ask if I get lost on the internet.
- I can send and open emails together with my teacher.
- I can write polite and friendly emails to people that I know.
- I will not tell anyone my username and password apart from my parents and teacher.
- I know that the school can look at anything I do on the computers.
- I understand that if I break these rules, I could be stopped from using the school site or computers

The following rules apply to Key Stage Two pupils:

- I will ask permission before entering any web site, unless my teacher has already approved that site.
- I will only use my own login and password, which I will keep secret.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send will be polite and sensible.

- I can use Google Classroom sensibly through my posts about my work and others by responding in documents (e.g., Google Docs), on the class stream and in any other threads.
- I can use Google Classroom appropriately inside and outside of school, for example during remote learning.
- When sending an e-mail, I will not give any information about myself or my family, including my home address or phone number.
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- If I see anything I am unhappy with, or I receive messages I do not like, I will tell a teacher immediately.
- I will only use the school site to talk to people I know in my school unless my teacher has said otherwise.
- I know that the school can look at anything I do on the computers.
- I understand that if I break these rules, I could be stopped from using the school site, the internet or computers
- I know that the school may check my computer files and may monitor the Internet sites I visit.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.

These rules will be clearly displayed in the ICT suite and by all classroom computers.

5.1.1 Sanctions

1. Violations of the above rules will result in a temporary or permanent ban on Internet use. If a permanent ban is issued, parents will be notified.
2. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
3. When applicable, police or local authorities may have to be involved.

5.2 Staff

All staff are asked to use the Staff Acceptable Use Agreement.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the headteacher

6) Policy Decisions

6.1. Authorising Internet access

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.
- Pupils will be informed that Internet use will be monitored.
- All users must read, sign and abide by the 'E-Safety Policy' before using any school Computing resource.

6.2. Assessing risks

- 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. Neither the school nor Solihull LA can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit the computing planning and curriculum to establish if the e-safety policy is adequate and that its implementation is effective.

6.3. Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher, who should use the agreed SMBC procedures.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Complaints of cyber bullying are dealt with in accordance with our anti-bullying policy.

6.4. Community use of the Internet

- The school will liaise with local organisations to establish a common approach to E-safety.

7) Communications Policy

7.1. Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.
- The E-safety policy will be referred to in all the units of the Computing curriculum, where appropriate e.g. in communication units.

7.2. Staff and the e-Safety policy

- All staff will be given the School E-Safety Policy and its importance will be explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- All staff should be familiar with the school's policy including safe use of email, internet including instant messaging, safe use of school network, equipment and data, safe use of digital images and digital technologies e.g. mobile phones and digital cameras, e-bullying/cyber bullying and their role in e-safety education for pupils.

7.3. Enlisting parents' support

- Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school Web site.
- A partnership approach with parents will be encouraged. This could include parents' evenings with demonstrations and suggestions for safe home Internet use. In addition E-safety information is on the website for parents to access.

- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

7.4. Where and when does it apply

- Computing activities on school premises during core school hours.
- Computing activities on school premises during extended school hours.
- Use of educational portals or learning platforms provided by the school, whether inside or outside of school premises and hours, for example Google classroom.
- Live communications features provided by schools (Instant Messaging, web cams etc.)
- Email provided by schools, including web based.
- Electronic publishing, including school web sites, Blogs etc.
- Computing activities whilst out on educational visits

8) Personal or sensitive information

Protecting Personal, Sensitive, Confidential and Classified Information

Ensure that any school information accessed from your own PC or removable media equipment is kept secure

- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- Only download personal data from systems if expressly authorised to do so by your manager
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

9) Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such as Smartphones, Chromebooks, iPads, games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

9.1 Personal Mobile Devices (including phones) - staff

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device
- The phone should not be on in the classroom.
- Staff are not allowed to use smart devices linked to mobile phones such as watches, glasses and other similar devices.

9.2 Personal Mobile Devices (including phones) - pupils

- Pupils are not allowed to bring personal mobile devices/phones to school.
- Pupils are not allowed to use smart devices linked to mobile phones such as watches, glasses and other similar devices.

9.3 Personal Mobile Devices (including phones) – visitors to school

- Parents/visitors must not use their mobile phones whilst in the classroom or in the vicinity of the children. Visitors will be asked to turn off their mobile phones and for them to be out of sight of the children whilst in school. Information to this effect is displayed to inform visitors of our expectations. Please see the mobile device policy.
- Visitors are not allowed to use smart devices linked to mobile phones such as watches, glasses and other similar devices.

9.4 Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- Ensure removable media is purchased with encryption
- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Encrypt all files containing personal, sensitive, confidential or classified data
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

10) Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, harassing and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputy will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

11) Responding to online incidents and safeguarding concerns

- All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.
- All members of the school/setting community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.
- The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Complaints about online/cyber bullying will be dealt with under the School's anti-bullying policy and procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Pupils, parents and staff will be informed of the schools complaints procedure.
- Staff will be informed of the complaints and whistleblowing procedure.
- 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.
- 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.
- The school will manage online safety (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 as 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 Education Safeguards Team or Solihull Police via 101 or 999 if there is immediate danger or risk of harm.
- 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 to Solihull Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
- Parents and children will need to work in partnership with the school to resolve issues.

12) How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in this policy and our Behaviour Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct and disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12.1 Responding to concerns regarding Youth Produced Sexual Imagery or "Sexting"

- Oak cottage will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as "sexting").
- The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- Oak Cottage views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead, Mr R Marshall.
- If the school are made aware of incident involving creating youth produced sexual imagery the school will:
 - Act in accordance with the schools child protection and safeguarding policy and the relevant Solihull Safeguarding Child Boards procedures.
 - Immediately notify the designated safeguarding lead.
 - Store the device securely.
 - Carry out a risk assessment in relation to the children(s) involved.
 - Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
 - Make a referral to children's social care and/or the police (as needed/appropriate).
 - Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
 - Implement appropriate sanctions in accordance with the schools behaviour policy but taking care not to further traumatise victims where possible.
 - Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.
 - Inform parents/carers about the incident and how it is being managed.
- The school will not view an images suspected of being youth produced sexual imagery unless there is no other possible option or there is a clear need or reason to do so (in these cases the image will only be viewed by the Designated Safeguarding Lead).
- The school will not send, share or save content suspected to be an indecent image of children and will not allow or request children to do so.
- If an indecent image has been taken or shared on the school/settings network or devices then the school will take action to block access to all users and isolate the image.
- The school will take action regarding creating youth produced sexual imagery, regardless of the use of school/setting equipment or personal equipment, both on and off the premises.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

12.2. Responding to concerns regarding Online Child Sexual Abuse and Exploitation

- Oak Cottage will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- Oak Cottage views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead (Mr R Marshall)
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Solihull Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline) then it will be passed through to the CSET team by the DSL.
- If the school are made aware of incident involving online child sexual abuse of a child then the school will:
 - Act in accordance with the school's child protection and safeguarding policy and the relevant Solihull Safeguarding Child Boards procedures.
 - Immediately notify the designated safeguarding lead.
 - Store any devices involved securely.
 - Immediately inform Solihull police via 101 (using 999 if a child is at immediate risk)
 - Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse e.g. using the Click CEOP report form: www.ceop.police.uk/safety-centre/
 - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
 - Make a referral to children's social care (if needed/appropriate).
 - Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
 - Inform parents/carers about the incident and how it is being managed.
 - Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where necessary.
- The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
- The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If pupils at other schools are believed to have been targeted then the school will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.

12.3. Responding to concerns regarding Indecent Images of Children (IIOC)

- Oak Cottage will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- The school will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school/setting equipment or personal equipment, both on and off the premises.
- The school will take action to prevent access accidental access to of Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.

- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Solihull Police.
- If the school/setting is made aware of Indecent Images of Children (IIOC) then the school will:
 - Act in accordance with the schools child protection and safeguarding policy and the relevant Solihull Safeguarding Child Boards procedures.
 - Immediately notify the school Designated Safeguard Lead.
 - Store any devices involved securely.
 - Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF): <https://www.iwf.org.uk/report/>, Solihull police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).
- If the school are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet then the school will:
 - Ensure that the Designated Safeguard Lead is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
 - Ensure that any copies that exist of the image, for example in emails, are deleted.
- If the school are made aware that indecent images of children have been found on the schools electronic devices then the school will:
 - Ensure that the Designated Safeguard Lead is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
 - Ensure that any copies that exist of the image, for example in emails, are deleted.
 - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
 - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:
 - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
 - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
 - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
 - Follow the appropriate school policies regarding conduct.

12.4. Responding to concerns regarding radicalisation and extremism online

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils. (Schools will need to highlight specifically how internet use will be monitored either here or within previous sections)
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the safeguarding policy.
- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been

committed then the Designated Safeguarding Lead will obtain advice immediately via the Education Safeguarding Team and/or Solihull Police.

12.5. Responding to concerns regarding cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of the Oak Cottage community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.
- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Solihull Police.
- Pupils, staff and parents/carers will be advised to keep a record of cyberbullying 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 schools e-Safety ethos.
- Sanctions for those involved in online or cyberbullying may include:
 - Those involved will be asked to remove any material deemed to be inappropriate or offensive.
 - A service provider may be contacted to remove content if those involved refuse to or are 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 involved in online bullying will be informed.
 - The Police will be contacted if a criminal offence is suspected.

12.6. Responding to concerns regarding online hate

- Online hate at Oak Cottage will not be tolerated. Further details are set out in the school policies regarding anti-bullying and behaviour (links)
- All incidents of online hate reported to the school will be recorded.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures e.g. anti-bullying, behaviour etc.
- The Police will be contacted if a criminal offence is suspected. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Solihull Police.

13) Monitoring arrangements and review

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the E-safety coordinator. At every review, the policy will be shared with the governing board. The review (such as the one available [here](#)) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

14) Links to other policies

The school's E-safety policy will operates in conjunction with other policies including those for:

- Child Protection
- Computing
- Behaviour
- Health and Safety,
- Curriculum
- Mobile Device policy
- Data Protection and Security
- Social Media

Appendix 1.

Pupil's Acceptance of the School's Policy regarding Acceptable Use of the Internet

Please complete and return this form to your child's class teacher.

Your child will not be able to access the Internet or use email until this is returned.

Pupil's agreement:

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

I understand that if I break these rules then I may not be allowed to use the Internet.

Pupil's signature _____ Date ____/____/____

Parent's/Guardian's acknowledgement:

I have read and understood the school rules for responsible Internet use and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet, including email usage at home. I understand that the school is not liable for any damages arising from the use of Internet facilities.

I understand that I have responsibility for my child's use of the Internet outside school. I will try to ensure that my child understands the importance of keeping their password a secret,

Parent's/Guardian's signature _____ Date ____/____/____

Name of Pupil _____

Class _____

SCHOOL

The school acknowledges the above signatures and therefore grants Internet access.

Signed _____ (Head teacher)

Appendix 2.

Dear Parents/Guardians

Using the Internet at School

As part of our school's curriculum pupils will be provided with supervised access to the Internet. We believe that use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. They will be able to obtain a rich variety of resources from around the globe to enhance their studies as they research information from museums, libraries, educational organisations and a range of other suitable web sites. They will also learn to exchange e-mails with other pupils.

We take positive steps to mitigate against access to undesirable materials through the use of Solihull LA's internet service provider which filters the content available to schools. 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. Neither the school nor Solihull LA can accept liability for the material accessed, or any consequences of Internet access.

Children will be introduced to a set of rules and taught how to use the Internet responsibly within their computing curriculum. When they are given access to the Internet they will be supervised and directed towards specific curriculum activities and suitable web sites. However, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The school will not be liable for any damages arising from your child's use of the Internet facilities.

Should you wish to seek further information regarding Internet use, you may find the following web sites and contact numbers useful:

(<http://www.safety.ngfl.gov.uk>)
UK Online - 0800 77 1234
<http://www.wiseuptothenet.co.uk>
<http://www.thinkuknow.co.uk>

A copy of the school's E-Safety Policy can be viewed on our website.

I enclose a copy of the schools' rules for using the Internet (appropriate to their key stage) which I would ask you to read and acknowledge by signing the enclosed slip for return by

.....

Should you wish to discuss any aspect of our use of the Internet please telephone me to arrange an appointment.

Yours sincerely

MR C SWAIN

Computing co-ordinator

Appendix 3

Acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date:

Appendix 4:
Online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	