Oakham Primary School

E-Safety and Acceptable Use Policy

Approved by Governors on:	**09/09/25**
Signature of Chair of Governors:	
Lead Personnel:	**S Stretton**
Date to be reviewed:	**09/09/26**

Rationale

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the real world.

Increasingly, children are accessing material through the internet and games consoles which is not age appropriate. It is essential to address this and to encourage a lifestyle which incorporates a healthy balance of time spent using technology.

This policy, supported by the Acceptable Use Policies (AUP) for staff, governors, visitors and pupils (see Appendix 1), is to protect the interests and safety of the whole school community and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies: child protection, digital images, health and safety, behaviour and PSHE.

Both this policy and the Acceptable Use Policies (for all staff, governors, visitors and pupils – see Appendix 1) are inclusive of both fixed and mobile internet, technologies provided by the school (such as PCs, laptops, whiteboards, voting systems, digital video equipment, etc) and technologies owned by pupils or staff.

The Technologies

Computing in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- E-mail
- Instant Messaging including within apps
- Blogs
- Social Networking Sites
- Chat Rooms
- Gaming Sites
- Text Messaging and Picture Messaging
- Video Calls
- Online Communities Via Games Consoles

Whole School Approach to The Safe Use of ICT

Creating a safe computing learning environment includes three main elements at this school:

- An effective range of technological tools which are filtered and monitored.
- Policies and procedures, with clear roles and responsibilities.
- A comprehensive E-Safety education programme for pupils.

The school believes that the benefits to pupils from access to the Internet far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians. This is why we ask both pupils and parents to

sign a copy of the pupil Acceptable Use Policy, which is stored with the child's admission records.

At Oakham, we feel that the best recipe for success lies in a combination of site-filtering, supervision and by fostering a responsible attitude in our pupils in partnership with parents.

Using the Internet for Education

The school intends to teach pupils about the vast information available on the Internet, using it as a planned part of many lessons. With the wireless network, access to the Internet can take place throughout the school at any time, ensuring web-based materials can be utilised to maximum efficiency.

All staff will review, evaluate and share resources available on web sites appropriate to the age range and ability of the pupils being taught. The Computing Lead will assist in the dissemination of this information using the termly unit plans.

If staff find any issues with the use of the internet, they need to report these to the ICT technician immediately – especially if the issues are regarding E-Safety.

Children may be given tasks to perform using a specific group of web sites. Sometimes, pupils may use a child-friendly search engine such as FactMonster, SafeSearch, KidRex etc to find appropriate images or web-based information. Tasks will be set to encourage pupils to view web sites and information with a critical eye, challenging the authenticity and validity of non-trusted websites.

Pupils' Access to the Internet

Oakham will use Sonicwall's 'filtered' Internet Service, which will minimise the chances of pupils encountering undesirable material. If any materials are found by pupils or staff which are deemed inappropriate, these must be reported to the ICT technician as soon as possible so that the content can be made aware of and blocked as necessary.

Oakham will only allow children to use the Internet when there is a responsible adult present to supervise. However, it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen, so there is an element of trust with all children when the internet is being used. If children are using the internet irresponsibly, then children may be asked to stop using the internet for a period of time (depending on the reason they have been asked to stop).

Members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils, the expectation we have of them. Web-based teaching materials will be built into ICT schemes and class assemblies to reinforce key online safety messages. Parents will be supported with web-safety updates; workshops when needed and links to useful websites. Teachers and School Leaders will continue to support E-Safety messages across school to spread the message to the rest of the children.

Expectations of Oakham Pupils Using the Internet

At Oakham, we expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access and language they use.

Pupils using the internet are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the IT technician can block further access to the site.

Pupils are expected not to use any rude language in their email communications and contact only people they know or those the teacher has approved. They are taught the rules of etiquette in email in KS2 (younger pupils are not granted access to emails) and are expected to follow them.

Pupils must ask permission before accessing the Internet and have a clear idea why they are using it. Pupils should not access other people's files unless permission has been given by the class teacher. Computers should only be used for schoolwork and homework unless permission has been granted otherwise.

No program files may be downloaded to the computer from the Internet. This is to prevent corruption of data and avoid viruses.

No storage devices may be brought into school on disc or memory stick but the class teacher may obtain data through consultation with the IT Technician.

No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.

Web cameras will not be used as standard in school, unless as part of a specific activity or work unit under strict adult supervision and only if the adult has checked the contact first.

Pupils are aware that school-based email and internet activity is monitored and can be explored further if required

Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to Internet resources. They will also come under the general discipline procedures of the school alongside the school behaviour policy.

Pupils will be asked to sign the school user Acceptable Use agreement, ensuring that they are aware of expectations. Parents will also need to sign copies of this agreement and will be expected to shadow these rules for their children’s safety at home. All children in school will have been given a copy of this from N – Y6. The Acceptable Use Policy is stored with the child’s admission records.

Staff Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the policy is implemented and compliance with the policy is monitored. All staff are encouraged to create a talking culture in order to address any E-Safety issues which may arise in classrooms on a daily basis.

The responsibility for E-Safety has been designated to a member of the SLT – Deputy Headteacher

Our E-Safety Coordinator ensures they keep up to date with E-Safety issues and guidance through liaison with the LA and through organisations such as The Child Exploitation and Online Protection (CEOP) and BECTA. The school's E-Safety Coordinator ensures the Head, senior management and governors are updated as necessary.

Staff Awareness and Access to the Internet

All staff receive regular information and training on E-Safety issues in the form of in-house training and meeting time when needed. New staff receive information on the school's Acceptable Use Policy as part of their induction.

All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community.

All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas and through a culture of talking about issues as they arise.

E-Safety records of concern are recorded on MY CONCERN and are completed by staff as soon as incidents occur. They are reported directly to the school's designated safeguarding team.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school E-Safety procedures. These behaviours are summarised in the AUPs which must be signed and returned before use of technologies in school.

Staff should email school-related information using their Office 365 address and not personal accounts. Staff will preview any websites before recommending to pupils. Suitable websites will be provided on class pages by staff for children to use.

The CEOP Report Abuse button is available on the school website. Teachers make children aware of this and when it is appropriate to use it.

Staff are aware that school-based email and internet activity is monitored and can be explored further if required. Staff should also be aware that all school devices are subject to the same filtering and monitoring processes regardless of location of use. Please see the filtering and monitoring protocol for further clarification.

Staff should only install software that the IT Technician has checked and approved and should report any spam or phishing emails that are not blocked or filtered.

At the end of the day, devices should be shut down and staff should try to prevent people from watching passwords being entered or viewing sensitive information.

Members of staff who repeatedly breach the acceptable use policy may face disciplinary action. A misuse or breach of this policy could also result in criminal or civil actions being brought against you.

Passwords

- Use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers).
- Passwords should be easy to remember but hard to guess.
- Passwords should not be written down.
- Passwords should not be shared with other children or staff.

Mobile Technology (laptops, iPads, netbooks, etc)

Staff are responsible for school devices outside of school and should not let unauthorised people use laptops/tablets for personal use.

Staff laptops should not be left in cars. If this is unavoidable, it should be temporarily locked out of sight in the boot. Mobile technology for pupil use, such as iPads and netbooks, are stored in a locked cupboard. Access is available via the school office key holders. Members of school staff (not visitors or children) should sign in/out the technologies before and after each use.

No personal devices belonging to children are to be used during lessons at school. If staff bring in their own devices such as mobile phones, these are to be used during break times only and kept on silent.

If pupils bring in mobile phones (for the purpose of safety if they walk to and from school alone), they should be kept switched off and sent to the office during the day. Any children not following these rules will be dealt with using the school's behaviour policy.

Within the Early Years Setting at our school and to ensure the safety and welfare of our children in our care; personal mobile phones are not permitted within this setting, when in the presence of children. This being a statutory requirement of the Early Years Foundation Stage Framework. (See Appendix 2)

Therefore, we will ensure that the setting takes measures including:

1. All mobile phones must be kept in a secure place and should not be accessed throughout contact time with the children.

2. Photographs or images of any children within our care may only be taken following parental consent and only using the school camera/phone and those images should remain within the setting.

3. When on outings, mobile phones may only be used to make or receive phone calls relating directly to ensuring the safety and wellbeing of the children.

Data Storage

Encrypt all removable media (USB pen drives, CDs, portable drives) taken outside school or sent by post or courier. No sensitive data should be stored on staff laptops (such as photos, IPPs and pupil information).

Sensitive data such as SEND/ assessment records, pupil medical information and any other data related to pupils or staff should not be stored on personal memory sticks but stored on

an encrypted USB memory stick provided by school, or on our secure Office 365 learning platform in the staff area. They should only be used with school devices and not be used on any public computer system or network.

Resources can be stored on non-encrypted memory sticks providing that they do not contain any information about the children, staff or school.

Social Networking Sites

- Use such sites with extreme caution, being aware of the nature of what you are publishing online in relation to your professional position.
- Under no circumstances should present or past school pupils be added as friends.
- Staff should be mindful about what they put on social media sites (both photos and posts), ensuring that they maintain a level of professionalism at all times (especially if they are friends with friends of parents).
- Make sure that any profiles are kept private to eliminate the chances of information being leaked.
- Under no circumstances should any reference to pupil's name or work be made on any social network site.
- Under no circumstance should any images of school children be used on social networks, including images in the background of other images.
- Any photographs taken inside school should not make the school identifiable and should certainly not show any pupils.

Digital Images

- Use only digital cameras and video cameras provided by the school and under no circumstances use personal camera phones to store images of children.
- Ensure you are aware of the children whose parents/guardians have not given permission for their child's image to be used in school. An up-to-date list is kept on the SIMS system. This is also given out to class teachers as needed.
- When using children's images for any school activity, they should not also be identified by their full name.

Providing A Comprehensive E-Safety Education to Pupils and Parents

All staff working with children must share a collective responsibility to provide E-Safety education to pupils and to promote E-Safety in their own actions. Formally, an E-Safety education is provided by the objectives contained in the Computing unit plans for every area of work for each year group. Even if E-Safety is not relevant to the area of Computing being taught, it is important to have this as a 'constant' in the Computing curriculum.

Informally, a talking culture is encouraged in classrooms which allows E-Safety issues to be addressed as and when they arise. The Deputy Headteacher will lead an assembly (alongside other teaching staff) on Safer Internet Day, highlighting relevant E-Safety issues and promoting safe use of technologies.

All classes will focus on E-Safety at least once per year, during which their class teacher will lead lessons and activities designed to educate children in keeping safe when using the internet and other new technologies.

Staff will ensure children know to report abuse using the CEOP button widely available on many websites, or to speak to any member of staff, who will escalate the concern to the Computing Subject Champion with responsibility for E-Safety.

When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's computing guidelines (see appendix 1). Children will be encouraged to educate parents through both classroom activities and homework-based activities when possible.

Complaints Procedure

As with other areas of school, if a member of staff, a child or a parent/carer has a complaint or concern relating to E-Safety, then they will be considered and prompt action will be taken. Complaints should be addressed to the Deputy Teacher in the first instance, who will undertake an immediate investigation and liaise with the leadership team and those members directly involved.

Incidents of E-Safety concern will be recorded using MY CONCERN and reported to the school's designated safeguarding team in accordance with school's child protection policy. Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

Appendix 1: **Oakham Primary School**

Computing Acceptable Use Policy for pupils for use at home (H) and at school (S).

The school has installed computers and Internet access to help our learning.

These rules will keep us safe and help us to be fair to others.

- I will only use computers in school for school purposes. (S)
- I will ask permission from a member of staff before using the Internet and will only be online when an adult is in the room. (S)
- I will only use my login and password and never share these with others. (S) (H)
- I will ask permission before bringing in memory sticks or CD ROMs into school. (S)
- I will only open and delete my own files. (S)
- The messages I send will be polite and sensible. (S) (H)
- I will never give out my own or other people's name, address or phone number online. (S) (H)
- I will never upload any images of school activities to any social networking site. (S) (H)
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. (S) (H)
- If I see anything I am unhappy with on the computers, I will turn the screen off and tell my teacher or an appropriate adult straight
- away. (S) (H)
- I understand that the school can check my computer use and that my parents/carers can be contacted if school staff are concerned about my E-Safety. (S)

Pupil Name		Class:
Pupil Signature		Date:
Parent/Carer Name		
Parent/Carer Signature		Date:

Oakham Primary School

Computing Acceptable Use policy for Staff, Governors and Visitors

These rules are designed to protect staff and visitors from E-Safety incidents and promote a safe e-learning environment for pupils.

- I will only use the school's internet, email, computers, laptops and mobile technologies for professional purposes as required by my role in school.
- I will not disclose my password to anyone outside of school.
- I will ensure that any online communications with staff, parents and pupils are compatible with my professional role.
- I will not give out my own personal details to pupils or parents.
- I will send school business emails using my school email address, if I have been provided with one, not my personal email address.
- I will ensure any data that I store is stored on a secure, encrypted device.
- I will not browse, download, upload or distribute any material which could be considered offensive, illegal or discriminatory.
- Images of pupils will only be taken and used for professional purposes in line with school policy with consent of the parent or carer and not distributed outside of school without the permission of the parent/carer and Headteacher.
- If it is necessary to bring my own personal devices into school, these will only be used during non-contact time without pupils.
- I will report any E-Safety concerns to the designated safeguarding officer immediately using My Concern.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support the school's E-Safety and Acceptable Use policy and help pupils to be safe and responsible in their use of technology.
- I understand that my online activity and use of school devices will be subject to regular review as per the filtering and monitoring protocol.

I understand the procedures and guidance above and agree to follow them with immediate effect.		
Name:	Signed:	Date:

Appendix 2

This room is a MOBILE PHONE * FREE ZONE

Please leave your device in the storage box in the medical room and collect it when you leave.

*This also includes personal tablets, smart devices, cameras and recording devices.

For further information, please refer to our Safeguarding & Mobile Phone Policies.

Thank you for your co-operation