**E-Safety and Acceptable Use Policy**

**URGENT CONCERNS**

 If you have an immediate eSafety concern, please report it to the Head Teacher or a DSL. This may be done orally in the first instance to ensure speed of response but should be backed up by recording the incident using the Incident report form at the earliest opportunity

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include: Websites, Learning Platforms and Virtual Learning Environments, Email and Instant Messaging, Chat Rooms and Social Networking, Blogs and Wikis, Podcasting, Video Broadcasting, Music Downloading, Gaming, Mobile/Smart phones with text, video and/or web functionality, other mobile devices with web functionality.

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, is not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

 At Langar Church of England Primary School, we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. This eSafety and Acceptable Use Agreement is inclusive of fixed and mobile internet technologies provided by the school (such as PCs, laptops, webcams, whiteboards, digital video equipment, etc.) Disclaimer: Due to the constant changes taking place within technology, this policy may not contain the most recent developments. We will however, endeavour to share any important issues via our website.

**Roles and Responsibilities**

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The role of eSafety co-ordinator in our school is taken by the Computing Subject Leader. All members of the school community have been made aware of who holds this post.

 It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Nottinghamshire LA, CEOP (Child Exploitation and Online Protection) and Childnet. Senior Management and Governors are updated by the Head/eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

 It is the responsibility of the Head Teacher to ensure that all users are made aware of this Acceptable Use Policy (AUP) and that systems are established to ensure all new, existing and potential users are aware of this AUP and have signed the appropriate agreements.

• Newly appointed and existing Staff will be required to sign to say that they have read this revised policy and will be required to sign the associated Acceptable Use Agreement before being allowed access to the NCC e-mail and Internet Service.

• New and existing Pupils will be required to sign the associated Acceptable Use Agreement before being allowed access to the NCC e-mail and Internet Service.

• All visiting staff requiring access to the Email and Internet NCC Service will be required to sign the Acceptable Use Agreement before being allowed access to the NCC e-mail and Internet Service.

 • Receiving staff will ensure all visitors to the school are made aware of the restrictions regarding the use of personal ICT technology with regard to Safeguarding and Data Protection before being allowed beyond the Office area.

It is the responsibility of all staff to remain alert for breaches of this AUP by pupils, contractors, visitors or temporary members of staff. Staff should report their concerns immediately to the Head Teacher or Assistant Head Teacher, before the person leaves the premises in the case of visitors or temporary staff. This may be done orally in the first instance to ensure speed of response but should be backed up by recording the incident using the Incident report form (Appendix 3), available in Resources on the server, at the earliest opportunity.

This policy, supported by the school’s acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreement, behaviour (including the anti-bullying) policy and PHSE.

eSafety skills development for staff:

• Our staff receive regular information and training on eSafety issues in the form of staff meetings and notices.

• Details of the ongoing staff training programme can be found in the Computing co-ordinator file.

• New staff receive information on the school’s acceptable use policy as part of their induction.

• All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety 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 eSafety activities and awareness within their curriculum areas.

**Managing the school eSafety messages**

We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used. The e-safety policy will be introduced to the pupils at the start of each school year. Esafety posters will be prominently displayed. eSafety in the Curriculum

• The school provides opportunities within a range of curriculum areas to teach about eSafety.

• Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum.

• Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.

• Pupils are taught about copyright and respecting other people’s information, images, etc. through discussion, modelling and activities.

• Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues.

• Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher, trusted staff member, or an organisation such as Childline/CEOP report abuse button.

 • Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum

**Password Security**

All users read and sign an Acceptable Use Agreement (Appendices 1 and 2) to demonstrate that they have understood the school’s e-safety Policy. Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others. If you think your password may have been compromised or someone else has become aware of your password report this to the eSafety co-ordinator or Headteacher. Staff are aware of their individual responsibilities to protect the security and confidentiality of school network and assessment portal, including ensuring that passwords are not shared and are changed periodically.

**Data Security**

The accessing of school data is something that the school takes very seriously. Staff are aware of their responsibility when accessing school data. They must not:

• take copies of the data

• allow others to view the data

 • edit the data unless specifically requested to do so by the Headteacher and/or Governing Body.

 **Managing the Internet**

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. The use of the internet is monitored and internet filters are in place to ensure pupils are only accessing content that is appropriate to them. Whenever any inappropriate use is detected it will be followed up. The school maintains pupils will have supervised access to Internet resources (where reasonable) through the school’s fixed and mobile internet technology.

• Staff will preview any recommended sites before use.

• If Internet research is set for homework, it is advised that parents check the sites and supervise the work. Parents will be advised to supervise any further research.

 • All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

 • All users must observe copyright of materials from electronic resources.

**Infrastructure**

School internet access is controlled through the LA’s web filtering service. This system ensures high levels of filtering for all users to prevent access to inappropriate content, including material relating to terrorism and extremism.

• Langar Church of England Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998 Section 29 of the Counter-Terrorism and Security Act 2015.Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

• If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the teacher and then to the e-safety co-ordinator. It is the responsibility of the school, by delegation to the network manager at Nottinghamshire’s Edit helpdesk, to ensure that Anti-virus protection is installed on all school machines. This automatically updates.

 • Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school’s responsibility, nor the network managers to install or maintain virus protection on personal systems.

• Pupils are not permitted to download programs or files on school based technologies.

• If there are any issues related to viruses or anti-virus software, the e-Safety co-ordinator should be informed.

**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. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and smart phones are familiar to children outside of school too. 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.

Personal Mobile devices (including phones)

It is recognised that it is the enhanced functions of many mobile phones, smart watches, tablets and other communication devices that cause the most concern, and which are most susceptible to misuse. Misuse includes the taking and distribution of e.g. images of pupils/staff to other mobile phone users or email addresses or social media which could result in bullying or harassment. It is also recognised that mobile phones can cause an unnecessary distraction during the working day and can be intrusive when used in the company of others. When mobiles phones are misused it can impact on an individual’s dignity, privacy and right to confidentiality. Such concerns are not exclusive to children and young people; hence there is a duty to protect the needs and vulnerabilities of all. It is appreciated that it can be very difficult to detect when such devices are present or being used, particularly in relation to enhanced functions, such as cameras. The use of all mobile phones is therefore limited, regardless of their capabilities. The aim is to avoid distraction and disruption of the working day, and to minimise the opportunities for any individual to make any covert images or misuse functions in any other way. For the purposes of this policy please read ‘phone’ as any mobile phone, camera/smart phone, smart watches, tablets and other communication devices.

The school allows staff to bring in personal mobile phones and devices for their own use. Under exceptional circumstances, and with the knowledge of the head teacher, the school allows a member of staff to contact a parent/carer using their personal device. The school is not responsible for the loss, damage or theft of any personal mobile device. No image or sound recordings should be made on these devices of any member of the school community. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device. Mobile telephones and smart watches that are able to deliver text messages or receive calls, should not be used in the classrooms during the school day. Mobile telephone calls, short message services, etc. must never occur in the classrooms during contact time or with children present. The office staff will take emergency phone messages should they arise. Staff will only be called to the telephone during contact time in the case of an emergency. Personal devices can be used in the staffroom or offices during staff breaks.

 School provided Mobile devices (including phones)

Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used. Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

**Managing email**

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good “netiquette”.

The school gives staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed. It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business; personal e mail addresses should not be used

Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses. E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper. Staff sending emails to, parents are advised to cc. the Headteacher or Office. Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes. All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission, virus checking attachments. Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail. Staff must inform the eSafety co-ordinator or Head Teacher if they receive an offensive e-mail.

**Safe Use of Images**

Note: This section should be read in conjunction with the school’s Use of Images Statement.

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment

Consent of adults who work at the school

Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

Publishing pupils’ images and work

On a child’s entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways: on the school’s internet pages, in the school prospectus and other printed publications that the school may produce for promotional purposes, in display material that may be used in external areas, i.e. exhibition promoting the school general media appearances, e.g. local/national media/press releases sent to the press highlighting an activity (sent using traditional methods or electronically). This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child’s circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time. Pupils’ names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils’ full names will not be published.

**Storage of Images**

• Images/films of children are stored in the ‘resources’ area on the school server.

• Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Head Teacher.

• Rights of access to this material are restricted to the teaching and support staff within the confines of the school network.

Webcams

 • We do not use publicly accessible webcams in school.

• Webcams in school will only ever used for specific learning purposes and never using images of children or adults. Misuse of the webcam by any member of the school community will result in sanctions (as listed under the “inappropriate materials” section of this document).

Video Conferencing

Permission is sought from parents and carers if their children are involved in video conferences with end points outside of the school. All pupils are supervised by a member of staff when video conferencing. Approval from the Head Teacher is sought prior to all video conferences within school. The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences. No part of any video conference is recorded in any medium without the written consent of those taking part. Additional points to consider:

• Participants in conferences offered by 3rd party organisations may not be DBS checked.

 • Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

**Safe and Responsible Use of Social Networking Internet Sites**

Social Networking sites have dominated the internet and are used by a wide range of users worldwide. Whilst these sites are not appropriate for pupils in the primary age phase and thereby are not permitted in school, staff should ensure that if they are using sites of this nature or any other associated forums, that under no circumstances should work-related matters be discussed. This is to ensure that people are protected and to minimise the risk of breaching confidentiality and preventing cyber bullying amongst adults.

Although the school supports the right for staff to have a private life, caution should be taken when liaising with any person who is connected with the school. On Social Networking sites, where ‘friend’ requests can be sent and received (e.g. Facebook), staff members should not add any past or present pupils to their Facebook or other Social Network site personal page. Any ‘friend’ requests from children should be ignored and this should be brought to the attention of the Head Teacher who will alert the parents/carers. New Social Networking ‘connections/friend requests’ must not be made with parents who have children currently in school. A great deal of caution should also be used when ‘friending’ parents and carers of ex-pupils on Social Network sites, irrespective of friendships offline.

During conversations or wall posts or any other means of communication on Social Network sites (including WhatsApp groups), staff should not mention anything that may bring the school or the profession into disrepute. The school will apply the necessary disciplinary procedures to any breach of this policy. For further details on confidentiality and child protection, please refer to the relevant school policies (Confidentiality Policy and Child Protection Policy).

**Personal Use**

The main purpose for the use of email and Internet in schools is for teaching, learning, research, and approved business activities of the school. However, Langar Church of England Primary School allows limited personal use subject to the following limitations:

• The level of use is reasonable and not detrimental to the main purpose for which the service is provided;

 • Priority is given to the use of resources for the main purpose for which they are provided;

• Personal use is not of a commercial or profit-making nature, or for any other form of personal financial gain;

• Personal use is not connected with any use or application that conflicts with the users obligations to the school as their employer or as a pupil;

 • Personal use is not connected with any purpose or application that conflicts with the school’s rules, regulations, policies and procedures;

• Personal use complies with school’s policies and regulations.

**Misuse and Infringements**

Complaints

Complaints relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Incidents should be logged and followed up.

 Inappropriate material

 All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator. Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offence. Users are made aware of sanctions relating to the misuse or misconduct on the Acceptable Use Agreement.

**Equal Opportunities**

 Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools’ eSafety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

**Parental Involvement**

• Parents/carers and pupils are actively encouraged to contribute to the school eSafety policy by letter and by reporting unsuitable sites etc. to the eSafety co-ordinator.

• Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.

 • Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g. on school website).

• The school disseminates information to parents relating to eSafety where appropriate in the form of website postings and newsletter items.

 **Writing and Reviewing this Policy**

There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them. This policy will be reviewed annually and consideration given to the implications for future whole school development planning and new/emerging technologies.

Appendix 1

**Langar Church of England Primary School Acceptable Use Agreement/Code of Conduct: Staff, Governors and Visitors**

 ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school eSafety coordinator or the Headteacher.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

• I will only use the school’s email / Internet and any related technologies for professional purposes or for uses deemed reasonable by the Head or Governing Body.

 • I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

• I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

• I will not give out my own personal details such as mobile phone number and personal email address to pupils.

 • I will only use the approved, secure email system(s) for any school business.

• I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.

• I will not install any hardware or software without seeking permission from the Headteacher or eSafety Coordinator.

 • I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

• Images of pupils and/or staff will only be taken, stored and used for professional purposes in-line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Headteacher.

• I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher.

• I will respect copyright and intellectual property rights.

• I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

• I will support and promote the school’s e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature …….………………….…………………………… Date ……………………

Appendix 2

**Langar Church of England Primary School Pupil Acceptable Use Agreement/eSafety Rules**

• I will only use ICT in school for school purposes.

• I will not tell other people my ICT passwords.

• I will only open/delete my own files.

• I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.

• I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately.

 • I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone.

 • I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

• I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my eSafety.

**Advice for keeping safe:**

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school.

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online may not be telling the truth about who they are - they may not be a ‘friend’

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message, so do not open or reply.

-------------------------------------------------------------------------------------------------------------------------------------Dear Parent/Carer

 ICT including the internet, email and mobile technologies etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT. Please read and discuss these eSafety rules with your child and the guidance/ agreement for parents and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mr Owen-Jones (eSafety Coordinator)

We have discussed this and …………………………………….......................... (child’s name) agrees to follow the eSafety rules and to support the safe use of ICT at Langar Church of England Primary School.

Parent/ Carer Signature …….………………….…………………………. Class …… Date ……………………

Appendix 3

**Langar Church of England Primary School Parent Acceptable Use Agreement**

With access to rich dynamic content, connectivity across the globe, a platform for creativity and a place to engage in debate, digital technologies provide a powerful tool for learning. It is therefore essential that children are fully equipped to have the skills and knowledge to safely access and use digital technologies.

This Parent/Carer Acceptable Use Agreement is intended to help share the importance that the school places on keeping children safe with particular regard to online safety. It additionally intends to encourage parents/carers to be actively involved in their child’s online safety education, including encouraging transparent behaviour, critical thinking and reporting.

The school will aim to provide every child with the best access it can to online technologies. Filtering, monitoring and alert systems will be in place to help protect children from unnecessary risks. The school will actively encourage children to think critically about content and communication from others and develop strategies for recognising inappropriate content/behaviours and how to deal with them. In return, the school expects the children to demonstrate that they are responsible users of digital technologies at all times.

**We ask parents and carers to support us by:**

* Sharing and role modelling, good online behaviours with your child.
* Emphasising the importance of the Acceptable Use Policy and Agreement and the rules your child has agreed to.
* Highlighting the importance of accessing only age-appropriate content and sites along with the pitfalls of social media.
* Explaining how to keep an appropriate digital footprint.
* Discussing what is and isn’t appropriate to share online.
* Emphasising never to meet anyone online nor trust that everyone has good intentions.
* Reporting any concerns you have whether home or school based.
* Stressing the importance of openness when being online and that no one should ever be too ashamed or embarrassed to tell a trusted adult if they have seen/shared anything concerning or have had inappropriate online contact.
* Drawing up an agreement of online safety rules for outside of school that are applicable even when your child is at a friend’s home.
* Avoiding posting or replying to any comments about the school to social media (including WhatsApp groups) that may have a negative impact. Any concerns or worries should be reported to the school in the first instance.

Appendix 4

**Langar Church of England Primary School Incident Log**

|  |  |
| --- | --- |
| Date  | Time |
| Name (s) | URL(copy and paste the web address of the page concerned into this box)  |
| Machine/ Device being used (Be specific – serial number or location)  | Brief summary of incident  |
| Reported by(print name of staff member and sign) | Action Taken  |