# ST. NICHOLAS SCHOOL CHILD OKEFORD

## A CHURCH OF ENGLAND VOLUNTARY AIDED PRIMARY SCHOOL

**MISSION STATEMENT**
**Be the best you can be!**
*I can do all things through God who strengthens me.*
*Philippians 4:13*
Every voice heard, every day a new chance, everyone exploring opportunities.

---

# E-SAFETY POLICY AND ACCEPTABLE USE AGREEMENT

**(Combining iPad, Social Networking and Mobile and Electronic Devices Policies)**

## POLICY SUMMARY

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 children with the skills to access life-long learning and employment. This document sets out Child Okeford Primary School's policy and aims to achieve this.

| DATE ADOPTED | REVISION NUMBER | LAST REVIEW | NEXT REVIEW |
|---|---|---|---|
| July 2019 | 1 | | July 2020 |

**Contents** **Page**

1. **Introduction**

(1) 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 children with the skills to access life-long learning and employment.

(2) This document sets out Child Okeford Primary School's policy and aims to:

(i) Assist schools' staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.

(ii) Set clear expectations of behaviour and/or codes of practice relevant to digital technologies for educational, personal or recreational use.

(iii) Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

(iv) Support safer working practice.

(v) Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

(vi) Reduce the incidence of positions of trust being abused or misused.

(3) Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff in schools will always advise their Head teachers of the justification for any such action already taken or proposed. Head teachers will in turn seek advice from the Schools' HR team where appropriate.

(4) Information and Communications Technology (ICT) 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:

(i) Websites;

(ii) Learning Platforms and Virtual Learning Environments;

(iii) Email and Instant Messaging;

(iv) Chat Rooms and Social Networking;

(v) Blogs and Wikis;

(vi) Podcasting;

(vii) Video Broadcasting;

(viii) Music Downloading;

(ix) Gaming;

(x) Mobile/ Smart phones with text, video and/ or web functionality; and

(xi) Other mobile devices with web functionality.

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

(6) At Child Okeford School we understand the responsibility to educate our pupils in e-Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

(7) This policy is inclusive of both fixed and mobile internet; technologies provided by the school; (such as PCs, laptops, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobiles phones, camera phones and portable media players, etc).

(8) This policy should not be used to address issues where other policies and procedures exist to deal with them. For example any alleged misconduct which falls within the scope of the management of allegations policy requires the school to comply with additional child protection requirements as set out in that policy.
(9) The local authority is not able to accept liability for any actions, claims, costs or expenses arising out of a decision not to follow this recommended policy and its guidance, where it is found that the governing body has been negligent or acted in an unfair or discriminatory manner in exercising its employment powers.
(10) This document does not replace or take priority over advice given by HR, the safeguarding unit or the school's codes of conduct, dealing with allegations of abuse, other policies issued around safeguarding or IT issues (email, ICT and data protection policies), but is intended to both supplement and complement any such documents. This guidance has been agreed with the trade unions.

## 2. Roles and responsibilities

(1) As e-Safety is an important aspect of strategic leadership within the school, the Head teacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-ordinator in our school is **Ms Jill Watson** who has been designated this role as a member of the Senior Management team. All members of the school community have been made aware of who holds this post. It is the role of the e-Safety coordinator to keep abreast of current issues and guidance through organisations such Dorset LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.
(2) The Head teacher/ e-Safety coordinator updates Senior Management and governors and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

## 3. Writing and reviewing the policy

(1) This policy, supported by the school's Acceptable Use Agreement for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies including those for ICT, Home-school agreements, Behaviour, Health and Safety, Child Protection, and PSHE policies including Anti-bullying.
(2) This policy takes account of employment legislation and best practice guidelines in relation to social networking in addition to the legal obligations of governing bodies and the relevant legislation listed at appendix C.
(3) Our e-Safety policy has been written by the school, in conjunction with advice from various bodies. It has been agreed by the Senior Management Team, Staff and approved by the Governing Body. The e-Safety policy and its implementation will be reviewed annually.

## 4. E-Safety skills development for staff

Our staff receive regular information and training on e-Safety issues through the coordinator at staff meetings. All staff have been 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. New staff receive information on the school's Acceptable Use Agreement as part of their induction. All staff are encouraged to incorporate e-Safety activities and awareness within their lessons.

5. **E-Safety information for parents/ carers**

Parents/ carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child. Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used on the school website. The school will send out relevant e-Safety information through newsletters, the school website, and the school prospectus.

6. **Community use of the internet**

External organisations using the school's ICT facilities must adhere to the e-Safety policy.

7. **Teaching and learning**

(1) Internet use will enhance learning:

(i) The school will provide opportunities within a range of curriculum areas to teach e-Safety. Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.

(ii) Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. 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 member of staff, or an organisation such as Childline/ CEOP.

(iii) The school internet access will be designed expressly for pupil use and will include filtering 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.

(iv) Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

(2) 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 should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

8. **Managing internet access**

(1) Information system security: 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. School ICT systems capacity and security will be reviewed regularly. Virus protection will be updated regularly. Security strategies will be discussed with Dorset Council.

(2) E-mail:

(i) Pupils may only use approved e-mail accounts on the school system.

(ii) Pupils must immediately tell a teacher if they receive offensive e-mail.

(iii) Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

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

(v) The forwarding of chain letters is not permitted.

(3) Published content and the school website: the contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal

information will **not** be published. The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

(4) Publishing pupil's images and work: written permission from parents or carers will be obtained before photographs of pupils are published on the school website. 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. Parents/ carers may withdraw permission, in writing, at any time. Photographs that include pupils will be selected carefully and **will not** enable individual pupils to be clearly identified, unless written permission has been given by a parent or carer. Pupils' full names will not be used anywhere on the Child Okeford school website, particularly in association with photographs. Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

(5) Photographs taken by parents/ carers for personal use: in the event of parents/ carers wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on social media and personal websites, e.g. school performances and assemblies etc. Parents/ carers will be asked to sign a form agreeing to this at the start of the school year and are reminded of this before performances.

9. **Social networking and personal publishing**

(1) The school will block/ filter access to social networking sites. Newsgroups will be blocked unless a specific use is approved. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location. Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals. Our pupils are asked to report any incidents of bullying to the school.

(2) School staff and social networking:

(i) Managing personal information effectively makes it far less likely that information will be misused.

(ii) In their own interests, staff need to be aware of the dangers of putting personal information onto social networking sites, such as addresses, home and mobile phone numbers or place of work. This will avoid the potential for pupils or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties.

(iii) All staff, particularly new staff, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and the school if they are published.

(iv) Staff should never 'friend' a pupil at the school where they are working on their social networking site.

(v) Staff should never use or access social networking sites of pupils and should never accept an invitation to 'friend' a pupil.

(vi) Confidentiality needs to be considered at all times. Social networking sites have the potential to discuss inappropriate information and employees need to ensure that they do not put any confidential information on their site

about themselves, their employer, their colleagues, pupils or members of the public.

(vii) Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, pupils or other individuals connected with the school, or another school, or Dorset Council could result in formal action being taken against them.

(viii) Staff are also reminded that they must comply with the requirements of equalities legislation in their on-line communications.

(ix) Staff must never post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring the school or Dorset Council into disrepute.

(x) Some social networking sites and other web-based sites have fields in the user profile for job title etc. If you are an employee of a school and particularly if you are a teacher, you should not put any information onto the site that could identify either your profession or the school where you work. In some circumstances this could damage the reputation of the school, the profession or the local authority.

(3) Communication between pupils/ school staff:

(i) Communication between pupils and staff, by whatever method, should take place within clear and explicit professional boundaries.

(ii) This includes the wider use of technology such as mobile phones, text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs.

(iii) It is the expectation that the school should provide a work mobile and e-mail address for communication between staff and pupils. Staff should not give their personal mobile numbers or personal e-mail addresses to pupils or parents.

(iv) Staff should not request, or respond to, any personal information from a pupil, other than that which might be appropriate as part of their professional role.

(v) Staff should ensure that all communications are transparent and open to scrutiny. They should also be circumspect in their communications with pupils so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as 'grooming' in the context of sexual offending.

(vi) Staff should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/ carers.

(vii) E-mail or text communications between an adult and a pupil outside agreed protocols may lead to disciplinary and/ or criminal investigations. This also includes communications through internet based web sites. Internal e-mail systems should only be used in accordance with the school's policy.

10. **Staff use of personal devices**

(1) Staff are not permitted to use their own mobile phones and personal devices for contacting children.

(2) Staff should not use personal devices to take photos or videos of pupils and will only use school designated devices for this purpose. The only exception is where an external memory card is used to save images using a third party device such as a camera. That memory card must stay in school securely until all of the imaged have been wiped. If anyone sees someone using a personal device with a camera to take

images, this should be reported immediately to the nominated safeguarding person in the school. This is consistent with the safeguarding principle that if anything is seen that puts safeguarding at risk it should be reported immediately.

(3) Staff and volunteers should not use personal mobile phones and other electronic devices for personal reasons whilst they are responsible for children in teaching situations and in the playground. Staff may access their personal devices whilst off duty but not in designated areas used by children.

(4) On off-site visits, adults should ensure that they have access to a mobile phone and that this is switched on. These should only be used if there is an emergency of if they need to contact the school or other group leaders.

(5) Where staff members are required to use a mobile phone for school duties, for instance in the case of off- site activities, phone numbers will be recorded on the school risk assessment forms.

(6) If a member of staff needs to make an emergency call during teaching time, they must ensure the class is supervised and make or take the call in an appropriate area not designated for children.

11. **Social contact**

(1) Staff should not establish or seek to establish social contact via social media/ other communication technologies with pupils for the purpose of securing a friendship or to pursue or strengthen a relationship.

(2) There will be occasions when there are social contacts between pupils and staff, where for example the parent and teacher are part of the same social circle. These contacts however, will be easily recognised and openly acknowledged.

(3) There must be awareness on the part of those working with pupils that some social networking contacts, especially where these are not common knowledge, can be misconstrued as being part of a grooming process. This can also apply to social networking contacts made through outside interests or through the staff member's own family.

12. **Access to inappropriate images and internet usage**

(1) There are no circumstances that will justify adults possessing indecent images of children. Staff who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children is illegal. This will lead to criminal investigation and the individual being barred from working with children, if proven.

(2) Staff should not use equipment belonging to their school/ service to access any pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.

(3) Adults should ensure that pupils are not exposed to any inappropriate images or web links. Schools and schools' staff need to ensure that internet equipment used by pupils have the appropriate controls with regards to access. e.g. personal passwords should be kept confidential.

(4) Where indecent images of children are found by staff, the police and local authority designated officer (LADO) should be immediately informed. Schools should refer to the dealing with allegations of abuse against staff and volunteers policy and should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.

(5) Where other unsuitable material is found, which may not be illegal but which raises concerns about that member of staff, either HR or the LADO should be informed

and advice sought. Schools should refer to the dealing with allegations of abuse against staff and volunteers policy and should not attempt to investigate or evaluate the material themselves until such advice is received.

13. **Cyber bullying of staff**

(1) Cyber bullying can be defined as 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.'

(2) Prevention activities are key to ensuring that staff are protected from the potential threat of cyber bullying. All employees are reminded of the need to protect themselves from the potential threat of cyber bullying. Following the advice contained in this guidance should reduce the risk of personal information falling into the wrong hands.

(3) If cyber bullying does take place, employees should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or e-mails. Employees are advised to take screenshots of messages or web pages and be careful to record the time, date and place of the site.

(4) Staff may wish to seek the support of their trade union or professional association representatives or another colleague to support them through the process. Employees will also have access to the DC staff counsellor, subject to funding being agreed.

(5) Staff are encouraged to report all incidents of cyber bullying to their line manager or the head teacher. All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police.

14. **Managing filtering**

The school will work with the LA and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. If pupils or staff discovers an unsuitable site, it must be reported to the Class Teacher, e-Safety Coordinator or Head teacher. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

15. **Managing emerging technologies**

(1) Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. The use of portable media such as memory sticks and CD ROMS will be monitored closely as potential sources of computer virus and inappropriate material. Pupils are not allowed to bring personal mobile devices/phones to school. Any phones that are brought to school will be sent to the school office and kept there until the end of the day.

(2) The sending of abusive or inappropriate text messages outside school is forbidden. Staff will use a school phone where contact with pupils is required.

16. **Protecting personal data**

(1) The school will collect personal information about members of staff fairly and will let them know how the school and Dorset LA will use it. The school will use information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or guardians, if it is necessary, to pass information beyond the school or Dorset LA. The individuals concerned will be informed in advance if it is necessary to pass the information on to anyone else other than the school and Dorset LA.

(2) The school will hold personal information on its systems for as long as you remain a member of the school community and remove it in the event of your leaving or until it is no longer required for the legitimate function of the school. We will ensure that all personal information supplied is held securely, in accordance with the policies and practices of Dorset Council and as defined by General Data Protection Regulation 2018.

(3) You have the right to view the personal information that the school holds about you and to have any inaccuracies corrected.

17. **Policy decisions**

(1) Authorising internet access: pupil instruction in responsible and safe use should precede any Internet access and all pupils must sign up to the Acceptable Use Agreement for pupils and abide by the school's e-Safety rules. These e-Safety rules will also be displayed clearly in all networked rooms. Access to the internet will be by directly supervised access to specific, approved on-line materials. All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the internet in school by following the school's e-Safety rules and within the constraints detailed in the school's e-Safety policy. All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

(2) Password security: adult users are provided with an individual network and email login username and password, which they are encouraged to change periodically. Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others. Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS systems.

(3) 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 DC can accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT provision to establish if the e-Safety policy is adequate and that its implementation is effective.

(4) Handling e-Safety complaints: complaints of internet misuse will be dealt with by a senior member of staff and reported to the e-Safety coordinator. Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety coordinator and recorded in the e-Safety incident logbook. Any complaint about staff misuse must be referred to the Head teacher. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. Pupils and parents will be informed of the complaints procedure.

18. **Communication of policy**

(1) Introducing the e-Safety policy to pupils: e-Safety rules will be displayed in all classrooms and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PSHE lessons/ circle times/ anti-bullying week. Pupils will be informed that network and Internet use will be monitored.

(2) Staff and the e-Safety policy: all staff will be given the School e-Safety policy and its importance explained. Any information downloaded must be respectful of copyright, property rights and privacy. Staff should be aware that internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential. A laptop issued to a member of staff remains the property of the

school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to internet access, data protection and use of software, both in and out of school.

19. **School equipment**

(1) Staff/ Adult use of school designated devices:

(i) Only authorised school technology may be used to record children's activities.

(ii) On trips, staff and volunteers should only use school devices for the purpose of taking photographs/ videos.

(iii) In school, visitors accompanied by staff may be granted permission to use authorised devices for the purpose of recording work.

(iv) All staff are responsible for the location of electronic devices within their rooms. Devices which store data, children's information or photos must be locked away at the end of the day

(2) School iPads:

(i) Users must use protective covers/cases for their iPads.

(ii) See clauses 8(4) and 8(5) this policy for guidance on taking and use of images.

(iii) The iPad is subject to routine monitoring by Child Okeford School. Devices must be surrendered immediately upon request by any member of staff.

(iv) Users in breach of the Responsible Use Policy may be subject to further investigation including but not limited to; disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity. Child Okeford Primary School is not responsible for the financial or other loss of any personal files that may be deleted from an iPad.

20. **Safeguarding and maintaining the iPads as an academic tool**

(1) iPads are required to be charged and be ready to use in school.

(2) Items deleted from iPads cannot be recovered.

(3) The whereabouts of iPads should be known at all times.

(4) It is a user's responsibility to keep iPads safe and secure.

(5) iPads belonging to other users are not to be tampered with in any manner.

(6) If an iPad is found unattended, it should be given to the nearest member of staff.

(7) iPads should not be stored or left in unattended vehicles for example on school trips.

21. **Lost, damaged or stolen iPad**

(1) If an iPad is lost, stolen, or damaged, the ICT coordinator and Head teacher must be notified immediately. If the iPad is believed stolen the Head teacher will contact the police.

(2) iPads that are believed to be stolen may be tracked through iCloud. Users should not disable the find my device feature.

(3) Users removing their iPad from the school site accept liability for its loss or damage. They should ensure their personal home contents insurance covers school equipment.

(4) If an iPad is deemed to be lost negligently, school may seek to recover the costs of a replacement.

22. **Prohibited uses (not exclusive):**

(1) Accessing inappropriate materials – all material on the iPad must adhere to the ICT Policy outlined above.

(2) Illegal activities – use of the school's internet/ e-mail accounts for financial or commercial gain or for any illegal activity.
(3) Cameras – Users must use good judgment when using the camera. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way. Any use of camera in toilets or changing rooms, regardless of intent, will be treated as a serious violation.
(4) Images of other people may only be made with the permission of those in the photograph.
(5) Posting of images/ movies on the internet into a public forum is strictly forbidden, without the express permission of the Head teacher.
(6) Use of the camera and microphone is strictly prohibited unless permission is granted.
(7) Misuse of passwords, codes or other unauthorised access: users are required to set a passcode on their iPad to prevent other users from misusing it.
(8) Any user caught trying to gain access to another user's accounts, files or data will be subject to disciplinary action.
(9) Malicious use/ vandalism – any attempt to destroy hardware, software or data will be subject to disciplinary action.
(10) Jail breaking – jail breaking is the process of which removes any limitations placed on the iPad by Apple. Jail breaking results in a less secure device and is strictly prohibited.
(11) Inappropriate media may not be used as a screensaver or background photo. Presence of pornographic materials, inappropriate language, alcohol, drug or gang related symbols or pictures will result in disciplinary actions.
(12) Individual users are responsible for the setting up and use of any home internet connections and no support will be provided for this by the school.
(13) iPad users should be aware of and abide by the guidelines set out elsewhere in this policy.
(14) Child Okeford School reserves the right to confiscate and search an iPad to ensure compliance with this Responsible Use Policy.

23. **Breach of policy**

(1) If an adult breaches school policy, concerns will be taken seriously, logged and investigated appropriately.
(2) The Head teacher reserves the right to check the image content of staff's, parent's, visitor's or volunteer's mobile phone or other electronic recording device, should there be any cause for concern over the appropriate use of it. If inappropriate material be found, Child Protection procedures will be initiated.

24. **Monitoring and review**

(1) This policy is implemented on a day-to-day basis by all school staff and is monitored by the e-Safety Coordinator.
(2) This policy is the Governors' responsibility and they will review its effectiveness annually. They will do this during reviews conducted between the e-Safety Coordinator, ICT Coordinator, Designated Child Protection Coordinator, and Governor with responsibility for ICT and Governor with responsibility for Child Protection (e-Safety committee). Ongoing incidents will be reported to the full governing body.
(3) The IT policy will be revised by the e-Safety Coordinator.

Date for review: July 2020

Signed: …… (Head teacher)

Approved by the Policy Committee of Child Okeford School.

Signed: …… (Chair of Lynne Crighton)

Date:

This policy and our procedures have been developed in line with guidance from:
Keeping Children Safe in Education (2014)

Pastoral Care in schools: Promoting Positive Behaviour (2001) DFE guidelines 2014

| | |
|---|---|
| Policy written: Summer 2019<br>Review Date: July 2020 | Links to Child Okeford School policies:<br><br>Child Protection<br>Complaints procedures<br>Safeguarding<br>Behaviour<br>Whistleblowing |

**Appendix A**

PUPIL GUIDELINES FOR SAFE INTERNET

I will only use the Internet when there is a teacher present.

I will always ask for permission before accessing the internet /e-mail.

I will only use my own usernames and passwords to log on to the system and keep them secret.

I will not access other people's files.

I will only email people I know, or my teacher has approved and ensure that the messages that I send will be polite and responsible.

I understand that the use of strong language, swearing or aggressive behaviour is not allowed.

I will not give personal details (like my home address, telephone or mobile number), or the personal details of any other person to anyone, or arrange to meet someone unless my parent/carer or teacher has given me permission.

I will only download, use or upload material when I have been given the owner's permission.

I will only view, download, store or upload material that is lawful, and appropriate for other users.

If I am not sure about this, or come across any potentially offensive materials, I will inform my class teacher straight away.

I will avoid any acts of vandalism. This includes, but is not limited to, uploading or creating computer viruses and mischievously deleting or altering data from its place of storage.

Always quote the source of any information gained from the internet i.e. the web address, in the documents you produce.

Use the Internet for research and school purposes only.

I will not bring in memory sticks or CD Roms from home to use in school unless I have been given permission by my class teacher.

I understand that the school may check my computer files and may monitor the Internet sites that I visit.

I understand that if I don't follow these rules, my access to the school computer system may be suspended, and my parents/ carers will be informed.

**ST NICHOLAS PRIMARY SCHOOL**
**Acceptable Use Agreement**
**For Pupils**

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

| | | | |
|---|---|---|---|
| **Pupil's Name** | | **Class Teacher** | |
| As a school user of the Internet, I agree to follow the school rules on its' use. I will use the network in a responsible way and observe all the restrictions explained to me by my school. | | | |
| **Pupil Name (print)** | | | |
| **Pupil Signature** | | **Date** | |

| | | | |
|---|---|---|---|
| **Parents Name** | | | |
| As the parent or legal guardian of the pupil above, I give permission for my son or daughter to use the Internet. I understand that pupils will be held accountable for their own actions. I also understand that some of the materials on the Internet may be unsuitable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information. | | | |
| **Parents Name (print)** | | | |
| **Parents Signature** | | **Date** | |

**Appendix B**

ST NICHOLAS PRIMARY SCHOOL
Acceptable Use Agreement

For Staff

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school's E-Safety Policy has been drawn up to protect all parties – the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Staff requesting Internet access should sign a copy of this Acceptable Internet Use Statement and return it to the Head Teacher for approval.

All internet activity should be appropriate to staff professional activity or the student's education

Access should only be made via the authorised account and password, which should not be made available to any other person

Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden

Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received

Use for personal financial gain, gambling, political purposes or advertising is forbidden

Copyright of materials must be respected

Posting anonymous messages and forwarding chain letters is forbidden

As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media

Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden

Any breach of confidential data security MUST be reported immediately to the Head Teacher, or in their absence a member of the Senior Leadership Team. For example but not limited to, a compromise of password, laptop or USB data stick.

| | | |
|---|---|---|
| **Name** | | |
| **Date** | | **Signed** |

## Appendix C – Relevant legislation

Schools staff should be aware of the legislative framework which currently surrounds use of social media / communication technology in the UK. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

### Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

### GDPR 2018

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. This states that personal data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept longer than necessary;
- Processed in accordance with the data subject's rights;
- Secure;
- Not transferred to other countries without adequate protection.

### Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

### Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

### Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

### Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;

- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) and you arrange to meet them or travel to meet them (anywhere in the world) with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your

own gratification. It is also an offence for a person in a position of trust to engage in any sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

# ST. NICHOLAS SCHOOL CHILD OKEFORD

**A CHURCH OF ENGLAND VOLUNTARY AIDED PRIMARY SCHOOL**

# E-SAFETY POLICY AND ACCEPTABLE USE AGREEMENT

## SIGNATURE SHEET

Full Name: *(in block capitals)* _____

Office in the School or Role within it: *(e.g. teacher, TA, volunteer)*_____

_____

I sign below to confirm that I have read, understood and agree to the School's E-Safety Policy and Acceptable Use Agreement.

Signature: _____

Date: _____

*Please detach this page along the perforated line at the top and return to the School Office.*