THE PILGRIM SCHOOL

ICT Acceptable Use

POLICY

School Lead: Leader of Learning

Governor Lead: N/A

Last reviewed: 29 April 2015

Date of next review: 20 April 2020

Signed by Head teacher: _____ **Date**: _____

Policy for Safe and Acceptable use of Information and Communication Technology (ICT)

The Internet has enormous potential as a teaching and learning tool for both staff and pupils. Electronic information research skills are now a vital part of children's learning. However, there are problems and issues surrounding its use in school that need to be addressed. This policy is a response to those issues and problems and is intended to protect both staff and pupils.

PUPILS

Although filtering software is used and the school is part of the local LA intranet network, we cannot completely guarantee that pupils are unable to access unacceptable materials such as pornographic, racist, extremist political or violent material.

For this reason, it is essential to involve parents in sharing in the responsibility of protecting their children from undesirable materials. This involvement takes the form of a letter sent out to all parents of **pupils who will be using the Internet either at a designated base or on a laptop loaned to them by the school,** asking that they undertake to convey to their children their expectations with regard to using the Internet in a responsible and appropriate way. The letter includes an Internet Parent Permission Form, which must be completed and returned to school before pupils are allowed to use the Internet and e-mail at school. A copy of this is included in this policy statement. (**See appendix A)**

The school has developed a set of guidelines for Internet use by all pupils and these will be kept under review. Pupils are taught about how the Internet can empower them and help them. They are also told about potential problems surrounding the use of the Internet. Pupils who attend the school bases and use the school computers for Internet use will be reminded of the rules governing safe Internet use displayed in each learning room. (**See appendix B)**

As part of the PSHE lessons and tutorials students will be encouraged, advised and supported to take considered measures to keep themselves safe online by investigating, accessing and using safety settings with the world wide web E.G. Facebook settings.

There will always be adult supervision* of pupils who are working **on the Internet in the school bases.** The following points are emphasised in lessons and form the basis of guidelines for pupils:

1. Pupils may not use the Internet at school without permission from the teacher or without supervision
2. Pupils may not bring in memory storage from home to use on school computers. These may introduce viruses or may not be suitable
3. What is meant by unacceptable material
4. Material published on the Internet is not always helpful, true or reliable
5. There have been instances of adults pretending to be young people on the Internet
6. They must never give out information about themselves such as home address or telephone number unless a parent, carer or teacher has given permission
7. Pupils must report any unpleasant material or messages to an adult
8. Pupils are trusted to behave responsibly when using the Internet or e-mail
9. Pupils must always be polite in e-mails, and never reply to unpleasant messages
10. Internet pages viewed by pupils can be later retrieved. LCC and LCS and the teacher may do this to monitor the children's use of the Internet
11. Pupils must not use another person's password
12. Pupils in the school bases may not send an email that has not been checked by an adult

13. The guidelines for the use of mobile phones is set out in the Mobile Phone Appendix C
14. The use of social networking sites is not permitted on the Pilgrim sites unless permission is granted by a supervising teacher, and it follows the guidelines put in place by LCC's e safety policy Appendix D

Acknowledgements

The above document has some borrowed material from ACITT

*Supervision means being present in the room, though not necessarily actually watching what is on each monitor at all times.

STAFF

Acceptable Use by Employees of ICT Resources

The school provides information and communication (ICT) resources and services, to employees to assist them in the performance of their duties. Employees must abide by the rules and regulations relating to the use of ICT which are detailed in this document.

The rules are in place for the following reasons.

1. protection of staff from allegations of misuse
2. protection of staff from allegations via social networking sites
3. to minimise any legal challenge or criminal action.
4. to avoid any reduction in the efficiency of the official software, network and systems.
5. to reduce the risk of viruses entering the system.
6. to avoid the risk of offensive or illegal material being introduced into the system.

Use of PCs, laptops and Networks

Equipment is provided for work purposes and should have the software necessary for you to undertake your job. You should never load or access any software other than that which has been provided by the Network Manager.

Personal use.

Employees may use the ICT resources out of school hours for personal purposes provided that such use does not disrupt the system or harm the school's reputation and complies with all other school policies.

Specifically employees **may not** use the system for

1. any form of personal financial gain
2. any illegal activity
3. distributing chain letters, hoaxes or unsolicited mail
4. downloading, transmitting or displaying material that is inappropriate in a school
5. use personal email accounts or mobile phone numbers to contact pupils
6. transmitting or publishing information which is defamatory

7. any activity that breaches Lincolnshire County Council policies or procedures
8. transferring pupil information onto personal computers not owned by the school.

THE PILGRIM SCHOOL

DIGITAL IMAGERY AND PHOTOGRAPHY

Digital imagery and photographs are exciting media which can motivate and inspire pupils. We also think it is important to use photographs of our pupils enjoying the varied activities of their education while they are with us to promote the positive aspects of our work.
We use photographs in our internal publicity materials such as school brochures and booklets, on our displays, for staff training and assessment purposes and on our web site. From time to time, articles and photographs of special events will appear in newspapers.
To do all we can to ensure all photographs of our pupils are used correctly, we undertake to:

- Obtain parental permission to use photographs of their child/children, including newspaper publication
- Observe the County Council's guidelines on the use of photographs and video clips
- Only use photographs and images for the purposes stated above
- Store all electronic images securely and destroy them *within five years* of the child no longer receiving education provision from our school/service

We have a responsible approach to the use of digital imagery and photographs and hope that parents are able to support us in publicising the many positive aspects of our work.

Camera phones will NOT be used by any member of staff in this respect.

However, when working in settings such as homes where school equipment might not be available, camera phones may be used to record children's work providing the following conditions are met:

1. No other camera owned by the school is available
2. Written parental permission is given on each separate occasion (proforma provided)
3. A parent or adult carer is present during the photography
4. The child is not in the photograph unless prior permission has been sought as explained above.
5. Images are transferred at the earliest opportunity to a school device or folder and then deleted.

This policy is made available to all parents whose children are likely to be included in photographs or video clips (except where the pupil wishes to include an image of him or herself to include in the child's own work). The consent form below is used to ensure permission is received prior to any publication as defined above.

Parent / Guardian
I give permission for (insert staff name) to take a photograph(s) of my child/my child's work. I understand that this may be used for:

- Internal publicity e.g. displays; staff newsletters
- External publicity e.g. our website; newspaper articles about the work of the school
- Assessment and evidence of a child's work (which may be shared with their school)
- Staff training

(Please delete as appropriate)

Signed……Parent/ Guardian ……Date

The Pilgrim School

Agreement for Safe and Acceptable use of the Internet Appendix A

Dear (Parent / guardian)

Internet Permission Form

As part of their education provision at the Pilgrim School, pupils are offered supervised access to the Internet. Before using the Internet, pupils must obtain parental permission and both you and they must sign and return the enclosed form as evidence of your approval and their acceptance of school rules on this matter.
Access to the Internet will enable your child to access huge amounts of information and exchange messages with other Internet users and will support their learning in many ways. However, you need to know that some material accessible through the Internet is offensive, illegal, inaccurate and inappropriate. Despite using filtering software and linked to the LA intranet, and regardless of our policy of supervision, we cannot totally guarantee or take any responsibility that a child will not intentionally or unintentionally access unsuitable material.
We believe that the benefits to pupils from access to the Internet, in the form of information resources, outweigh any disadvantages.
Pupils will be taught in school about safe and acceptable use of the Internet and will be guided by teachers towards appropriate material. They will be periodically reminded of school rules with regard to using the Internet and the reasons for them. A copy of these is included. We ask that you, as parents, also discuss the issues with your child and convey the standards they should follow when using media and information sources at school and at home. We strongly recommend that parents refer to available advice about safe use of the internet and ensure that they are aware of any access that is taking place. Guidance is available from a number of websites, including Be Safe Online.
We would be grateful if you could complete the enclosed permission form and return it.

Yours sincerely
P. Squire
Leader of Learning

……

Internet Parent Permission Form
Please complete and return this form to school.
Pupil
As a school user of the Internet, I agree to abide by the school rules on its use. I will behave in a responsible way.

……Learner Signature ……Date

Parent / Guardian
I give permission for (insert name) to use e-mail and the Internet at school. I understand that the school cannot totally guarantee that objectionable material will not be seen and cannot be held responsible. I accept responsibility for setting standards for my child to follow when using the Internet.
Signed……Parent/ Guardian ……Date

Appendix B

The Pilgrim School

Rules for Responsible School Internet Use

Internet access can aid our learning. These rules will help keep everyone safe.

- Pupils may not bring in disks from home to use on school computers. These may introduce viruses or may not be suitable
- Never tell anyone you meet on the Internet your address or phone number
- Never send your picture to someone over the Internet
- Never arrange to meet anyone in person
- Always be yourself and do not pretend to be anyone or anything you are not
- Remember that you are on trust to use the Internet responsibly. Restrictions are set up by LCS which limits access to sites considered to be unsuitable or inappropriate, but you must not visit sites that you know are unacceptable
- Your internet access is monitored and every site you attempt to visit is recorded and may be traced back to you via the LCC and LCS system

Rules for acceptable and safe use of e-mail and other communication tools

- Use of communication tools (including e-mail) outside the Pilgrim School System remain the sole responsibility of the named adult.
- Pupils are only permitted to use e-mail and other communication tools once they have agreed to and signed this agreement.
- Use of Pilgrim School equipment, e-mail or internet for financial gain, political purposes or advertising is forbidden.
- You may only e-mail people the teacher has approved
- E-mails can be retrieved by the teacher and looked at later
- If inappropriate e-mail is sent, this may be recorded and may be traced back to you
- Any e-mail from unknown sources should be reported
- Saving or downloading materials is subject to guidance from the teacher Materials saved, downloaded or copied and pasted from the internet must not infringe copyright
- The school reserves the right to restrict or remove access in the event of any user misusing network and communication facilities
- The use of social networking sites is not permitted on the Pilgrim sites unless permission is granted by a supervising teacher, and it follows the guidelines put in place by LCC's e safety policy

Appendix C

Acceptable Use Mobile Phone Policy

Introduction:

The widespread ownership of mobile phones among young people requires that school administrators, teachers, pupils, parents and carers take steps to ensure that mobile phones are used responsibly at schools. This Acceptable Use Policy is designed to ensure that potential issues involving mobile phones can be clearly identified and addressed, ensuring the benefits that mobile phones provide (such as increased safety) can continue to be enjoyed by our pupils.

This policy sets out the School's framework governing what is deemed to be acceptable use of mobile phones. The purpose of this policy is to prevent unacceptable use of mobile phones or camera-phones, and thereby to protect the School's staff and pupils from undesirable materials, filming, intimidation or harassment.

It is recognised that these documents must be reviewed and revised regularly in response to the ever-changing ICT environment at the School. The Acceptable Use Policy for Mobile Phones also applies to pupils during school visits and extra-curricular activities.

The Policy:

The School understands a parent's wish for their child to have a phone for their journey to and from school. However, parents and pupils should understand that this is entirely at their own risk as the School accepts no responsibility for loss, theft or damage of any phone, mp3 player or device brought into school.

It is the responsibility of pupils who bring mobile phones to school to abide by the guidelines outlined in this document.

1. The School strongly advises that mobile phones should not be brought into school.
2. On a case by case basis determined by needs it may be possible to allow the mobile phone to remain in sight of the pupil during lessons and break times. However, in such cases, the mobile phone should remain turned to silent during school hours, including break and lunch times.
3. Any pupil wishing to use their mobile phone during school hours to make or receive a call, to send or receive texts, surf the internet, take photos or use any other application MUST first ask for permission from a member of staff.
4. The decision to provide a mobile phone to their children should be made by parents/carers.
5. Parents/carers should be aware if their child takes a mobile phone into school.
6. Pupils are responsible for keeping the school informed of their current mobile phone number.
7. Communications between parents and pupils during the school day should only occur through the School's official communication channels and not via a pupil mobile phone. Parents are expected to contact our main office or a member of staff whilst pupils wishing to contact home must ask permission to do so from a member of staff.

Unacceptable Use

1. It is forbidden to record photographic images (still or video) or sound recordings of staff or pupils without their explicit permission.

2. Using mobile phones to bully and threaten other students is unacceptable and will not be and will not be tolerated. In some cases it can constitute criminal behaviour.

   (It should be noted that it is a criminal offence to use a mobile phone to menace, harass or offend another person. As such, if action as sanctioned by the head teacher is deemed ineffective, as with all such incidents, the school may consider it appropriate to involve the police)

3. Under no circumstances should mobile phones be taken into any external examination. This includes those that are turned off within a bag or coat. Any pupil who is found in possession of a mobile phone will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.

Breach of the Policy

If any pupil is found to be **using their mobile 'phone without express permission from a member of staff**, we will regard this as a breach of the school rules.

Sanctions will be applied accordingly, the first of which will be that breaks must be taken indoors under staff supervision for the next 3 sessions.

If the action is repeated, pupils will be asked to hand in their 'phones until the end of the day.

Refusal will be regarded as a serious disciplinary matter and parents will be called to a meeting with a member of the senior leadership team to decide on further actions.

Any pupil who refuses to hand over a mobile phone when requested will be removed from lessons by a member of the senior leadership team and it will be treated as a disciplinary matter.

Advice on Safe Use of Mobile Phones

While the above policy has been drawn up as part of the school's behaviour and safety strategies, it is recognized that mobiles phones have recently become a common possession, are increasingly complex and sophisticated and can be great fun.
However, pupils need to be careful and keep safe. Advice on safe use of mobile phones will form part of the Induction programme and revisited, from time to time, within ICT and PSHE lessons.

Appendix D

Pages taken from the LCC E Safety Policy and Guide 2010
The whole document can be found in Pdf Format at:
http://www.cfbt.com/lincs/pdf/LCC%20policy%20and%20guidance1.pdf

E-Safety - responsibilities of schools staff

Information technologies are developing rapidly and can leave staff unsure of best practice or how to discuss e-Safety issues with pupils. Further advice can be sought from Lincolnshire Safeguarding, or from CfBT ICT consultants.

The trust between pupils and school staff is essential to education but very occasionally it can break down. This is not new, but has been highlighted by better awareness of human failings and greater respect for children. Nationally, CEOP was set up by the Home Office to "safeguard children's online experiences and relentlessly track down and prosecute offenders" and their work should be acknowledged and built upon by schools.

Within Lincolnshire a member of staff who flouts security advice or uses ICT technology for inappropriate reasons risks dismissal.

All staff should sign an Acceptable Use Policy on appointment. Staff thereby accept that the school can monitor network and internet usage to help ensure staff and pupil safety.

Staff that manage filtering systems or monitor ICT use have great responsibility and must be appropriately supervised. Procedures must define how inappropriate or illegal ICT use is reported to the Senior Leadership Team. Staff must be aware of dangers to themselves in managing ICT use, for instance in viewing inappropriate images to investigate their source.

Email, text messaging, Social Networking and Instant Messaging (IM) all provide additional channels of communication between staff and pupils. Inappropriate behaviour can occur and communications can be misinterpreted. Staff should be aware of the power of the Police to identify the sender of inappropriate messages. Schools should provide establishment email accounts for all staff.

Staff should be aware that students may be subject to cyberbullying via electronic methods of communication both in and out of schools. Head teachers should be aware that they have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site (Education and Inspections Act 2006) School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy (Education and Inspections Act 2006).

Any inadvertent access or allegation of inappropriate behaviour must be reported to the Senior Leadership Team and the DSO and investigated with care through liaison with appropriate authorities including LCS if required .

If there is any suspicion of illegal activity staff should NEVER investigate for themselves but must report to Lincolnshire Police as soon as possible.

E-Safety Policy (School Staff)

This policy has been created with a school emphasis using the e-safety policy of Lincolnshire Safeguarding Children's Board and the Acceptable Use of ICT Policy (AUP). This is a minimum requirement to which all school staff should adhere

Through whole school CPD, inset days and online training staff will have an up to date awareness of online safety matters and of the current school online safety policy and practices.

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues.
It is recognised that under certain circumstances inadvertent access may happen. For example, a school researching the holocaust may produce results with Nazi propaganda. Should you or a student access any of these sites unintentionally you should report the matter to a member of the Senior Management Team so that it can be logged and LCS our ICT provider.

Access to any of the following should be reported to Lincolnshire Police: images of child abuse (sometimes incorrectly referred to as child pornography). These are images of children apparently under 16 years old involved in sexual activity or posed to be sexually provocative; adult material that potentially breaches the Obscene Publications Act; criminally racist material in the UK.

Social networking - is blocked in our school until such a time as deemed appropriate by SLT and the Governing body

At any time social networking is allowed then the following should be implemented to ensure that there is strict policy with regards to security of personal details, rather than relying on the default settings. You should not name your place of work or use defamatory language or comments about colleagues, students or the school. Staff should fully acquaint themselves with the privacy settings that are available on any social networking profile in order that profiles are not publicly available.
At no time should staff be accessing social media sites on school provided networks or devices.

All digital communications with students / pupils/ parents/ carers should be on a professional level and only carried out using official school systems.

Members of staff should never knowingly become "friends" with students on any social networking site or engage with pupils on internet chat neither past nor current students. If a member of staff feels this status is appropriate it should be discussed with the head teacher and DSO before doing so.

Use of Email - All members of staff should use their professional email address for conducting school business.

Passwords - Staff should keep passwords private. Passwords are confidential and individualised to each person. On no account should a member of staff allow a student to use a staff login.

Data Protection - Where a member of staff has to take home sensitive or confidential information sufficient safeguards should be in place to prevent loss or misuse, i.e. is it really necessary to take it all home. Data should not be stored on pen drives or laptop hard drives as access should be gained through RDWeb server, and it should not be downloaded onto the individual device.

File sharing - technology such as peer to peer (P2P) and bit torrents is not permitted on the Lincolnshire School's Network.

Personal Use - Staff are not permitted to use ICT equipment for personal use if it contravenes any of the previous points.

Images and Videos - Staff and pupils should not upload onto any internet site images or videos of themselves or other staff or pupils without consent.

Use of Personal ICT - use of personal ICT equipment is at the discretion of the school. Any such use should be stringently checked for up to date anti-virus and malware checkers.

Viruses and other malware - any virus outbreaks are to be reported to the LCS as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

Staff should note that internet and email may be subject to monitoring

E-Safety Policy (students)

The use of ICT within schools has enormous benefits to education, however there are reasons why the school and the local authority must put some restrictions in place, such as: ICT equipment is very expensive to buy and maintain; the school and the local authority have a duty of care to ensure that you are safe and that you are not exposed to illegal or inappropriate content. It is hoped that these restrictions do not interfere with your education, but if you feel otherwise you are encouraged to talk to a member of staff to discuss any issues.

Please note that internet and email use may be subject to monitoring.

Use of the Internet - the internet is provided to help you with learning activities such as research, online activities, online educational games and many other things. The internet is not to be used to access any- thing which is illegal, or anything that someone else may find offensive. This would include pornography, discrimination, racial or religious hatred. If you are unsure, or if you come across anything you feel is inappropriate, you should turn your computer monitor off and let your teacher know. Never try to bypass the security by using proxy sites, these are all monitored.

Logins and Passwords - every person has a different computer login and password. You should never allow anyone else to use your details. If you think someone else may have your details you should have your password changed.

User Areas - your user area is provided for you to save school work. It is not to be used to save music or other files that you have brought in from home, nor should it be personalised by changing settings except in agreement of the case manager for accessibility reasons.

Social Networking - if social networking (for example Bebo, Facebook, Flickr) is allowed in your school you should never upload pictures or videos of others without their permission. It is not advisable to upload pictures or videos of yourself, videos and pictures can easily be manipulated and used against you. You should never make negative remarks about the school or anyone within the school. Always keep your personal information private to invited friends only and never post personal information such as your full name, date of birth, address, school, phone number etc. Consider using a nickname and only inviting people you know. Universities and future employers have been known to search social networking sites.

Beware of fake profiles and people pretending to be somebody else. If something doesn't feel right follow your instincts and report it to an appropriate adult. Never create a false profile as a joke and pretend to be somebody else. This can have serious consequences.

Some social networking sites have a chat facility. You should never chat to anyone that you don't know or don't recognise. It is recommended that you never meet a stranger after meeting them online. If you do, always inform your parents and take one of them with you.

Security - you should never try to bypass any of the security in place, this includes using proxy bypass sites. This security is in place to protect you from illegal sites, and to stop others from hacking into other people's accounts.

Copyright - you should never take information from the internet and use it as your own. A lot of information is copyright, which means that it is owned by somebody else and it is illegal to use this information without permission from the owner. If you are unsure, ask your teacher.

Etiquette - Our school provides students with email accounts. Always be polite and don't swear. Consider what you are saying, and how it might be read by somebody else. Without emoticons it is

difficult to show emotions in things like emails and blogs, and some things you write may be read incorrectly, this is monitored for safety.

Mobile Phones - Some modern mobile phones offer the same services as a computer, i.e. Facebook, YouTube, email access etc. This can be a great way of keeping in touch with your friends and family. But, in the same way that some internet services can be used inappropriately, the same is true with mobile phones.

School allows mobile phones in the classroom, these should not be used during the lesson unless your teacher has given you permission.

Never take inappropriate pictures of yourself or others and send to your friends or upload onto social networking sites. Never forward inappropriate pictures that you have received from somebody else. In some circumstances this can be an illegal act, nor should you request inappropriate images.

It is school policy that no photos of staff or pupils should be taken without prior agreement with the use being identified beforehand. This is due to not all students having photographic permission agreements in place at the time of induction.