Our Lady's Catholic Primary School

Loving, Learning and Reaching Out to All

Acceptable use of ICT and the Internet Policy & Procedure

Committee to approve/ratify policy	Full Governing Body
Policy Co-ordinator	Angela Sutton
Date of approval/ratification by Committee	11/10/22

Date for renewal	October 2023
Signature of the Chair of the Committee	

Mission Statement:

Overview

ICT equipment and the internet offer incredible opportunities for promoting and extending learning. In this school we will make best use of these tools to promote excellence and enjoyment. With the use of ICT and the Internet comes risk. We will do all we can to ensure that the internet and ICT is used safely and acceptably by all in school for the purposes that we intend. Staff and learners will be trained in acceptable use and the school will monitor usage.

Objectives

1. To ensure that on site and off site, ICT equipment and the internet are used in line with our E-safety and Safe Internet Usage Policies.
2. To ensure that all staff and learners understand what is acceptable use of ICT and the Internet related to teaching and learning and the curriculum.
3. To protect children from harm and upset that could be caused through accessing inappropriate sites, materials, images and contacts.
4. To make learners aware that there are inappropriate sites that are harmful and so must be avoided in school and at home.
5. To encourage learners to report immediately any inappropriate, sites, materials or contacts that they find on the internet either at school or at home.
6. To ensure that the school complies with section 127 of the communications Act 2003 and the recommendations of the Byron Report 2008.
7. To monitor devices to ensure that they have not been put to unacceptable use.
8. To ensure that all members of staff are personally responsible for acceptable use of any school equipment for which they are responsible.
9. To have a nominated member of the SLT, Mrs Sutton, who will have oversight of E-Safety, Acceptable Use of the Internet and Cyber Bullying.
10. To take immediate and prompt action to prevent misuse of ICT and keep a log of any e-safety issues or unacceptable usage (CPOMS)

Strategies

1. To train staff and learners in acceptable use of ICT and the Internet.
2. To monitor and supervise learners at all times when they use ICT and the internet.
3. Appropriate Firewalls will be put in place and must be enabled at all times on all the school computers.
4. Staff must always check that Firewalls are in place before learners are allowed to access the internet.
5. Staff must not disable or bypass Firewalls on any school owned computer under any circumstances or at any time.
6. To monitor staff usage of ICT equipment and the internet.
7. To ensure that all staff and learners understand that the school's ICT equipment must only be used for its intended purpose and not for personal use.
8. To only allow authorised persons to have use of the school's equipment.

9. School equipment must not be used for accessing personal and social networking sites.
10. Personal, portable storage devices must not be attached to school equipment.
11. Learners must be encouraged to notify staff if they at any time come across unsuitable material on a computer or if they feel threatened or harassed by any form of cyber bullying.
12. Staff must notify the headteacher immediately if they find unsuitable or inappropriate material on a computer or storage device or if they find that a learner is the subject of cyber bullying.
13. To take disciplinary action where this policy is breached and to take appropriate sanctions against those who breach it.
14. To act promptly if a discovery of inappropriate use found or if a disclosure is made.
15. To involve parents and any appropriate authorities where there is evidence of unacceptable use of ICT.
16. To ensure that passwords. ICT security and confidentiality are not breached and that all ICT is secure.
17. Staff must not use ICT to make social contact with pupils in this school or any other, nor should they allow any pupil to access to their personal or social websites in or out of school hours.
18. Pupils will not be allowed to have mobile ICT devices switched on whilst they are on school premises.
19. Staff must not display their personal mobile phones in class, use them in the presence of children and phones should be set to flight mode during lesson time.
20. Any cyber bullying of staff or pupils, in or out of school, must be reported and then investigated rigorously, in conjunction with school policy and any relevant authority, including the police if appropriate. Appropriate records will be kept (CPOMS).

Equal Opportunities and Inclusion
At Our Lady's Catholic Primary School we plan to provide for all pupils to achieve, including boys and girls, higher achieving pupils, gifted and talented pupils, those with SEN, pupils with disabilities, pupils from all social and cultural backgrounds including those who are Pupil Premium, Looked After Children and those who are subject to safeguarding, pupils from vulnerable groups and pupils from different ethnic groups and those from diverse linguistic backgrounds.

Outcome and impact
In this school we will do all that we can to ensure the acceptable use of ICT and the Internet to promote teaching, learning, excellence and enjoyment. This policy is written to promote the safety of all in our school.

1. Aims

The aims of this Acceptable Use Policy are:

- To ensure the safeguarding of all children and young people within and beyond the school setting by detailing appropriate and acceptable use of all online technologies.
- To outline the roles and responsibilities of everyone working with children and young people.
- To ensure adults are clear about procedures for dealing with misuse of any online technologies within the school setting.
- To develop links with parents/carers and the wider community ensuring their input into policies and procedures with continued awareness of benefits and potential issues of online technologies.

2. Roles and responsibilities of the school

2.1 Governors and Headteacher

It is the overall responsibility of the Headteacher and Governors to ensure that there is an overview of e-safety (as part of the wider remit of Child Protection) across the school with further responsibilities as follows:

- There is a focus on e-safety at the start of every year taught in each class from Y1 to Y6 by Mrs Dally linked to the CLC scheme. The teacher throughout the year will remind the children of the importance of remaining safe online.
- The co-ordinator is responsible for promoting e-safety across the curriculum and has an awareness of how this is being developed.
- The Head teacher will inform Governors at the curriculum meetings about the progress of or any updates concerning e-safety and ensure Governors know how this relates to Child Protection.
- The Governors must ensure Child Protection requirements are met including an awareness of e-safety and how it is being addressed within the school, as it is the responsibility of Governors to ensure that all Child Protection guidance and practices are embedded.
- Ensure that any misuse or incident has been dealt with appropriately, according to the policy and procedures and appropriate action is taken.

2.2 Staff or Adults

It is the responsibility of all adults within the school or other setting (including volunteers, consultants and contractors) to:

- Ensure that they know who the Designated Person for Child Protection is within the school or other setting so that any misuse or incidents which involve a child can be reported. Where an allegation is made against a member of staff it should be reported immediately to the Headteacher. In the event of an allegation made against the Headteacher, the Chair of Governors must be informed immediately. (Following the Inter Agency Safeguarding Procedures.)
- Be familiar with the Behaviour, Anti-Bullying and other relevant policies so that in the event of misuse or an allegation, the correct procedure can be followed immediately.
- Check the filtering levels are appropriate for their children and young people and are set at the correct level. Report any concerns to the E-Safety leader.
- Alert the e-safety leader of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children and young people are protected and supported in their use of online technologies and know how to use them in a safe and responsible manner so that they can be in control and know what to do in the event of an incident.
- Be up to date with e-safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998.
- Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- Report accidental access to inappropriate materials to the e-safety leader in order that inappropriate sites are added to the restricted list.
- Report incidents of personally directed ‘bullying’ or other inappropriate behaviour via the Internet or other technologies in the same way as for other non-physical assaults.
- Staff are not allowed to access anything other than educational sites
- Staff are not allowed to bring in or use their own personal laptops, tablets or USB sticks to use in school
- All USB sticks must be encrypted

All adults working with children and young people must understand that the nature and responsibilities of their work place them in position of trust.

2.3 Children and young people

Children and young people are:

- Taught to respect the equipment they use and made aware of the penalties for wilful damage.
- Taught to use the Internet across the curriculum in a safe and responsible manner through Computing, PSHE or other clubs and groups to minimise risks.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away.

3 Appropriate use by Staff and Adults

Staff members have access to the network so that they can access age appropriate resources for their classes and create folders for saving and managing resources. They have passwords to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.
When accessing the Learning Platform the same Acceptable Use Rules will apply. The acceptable use should be similar for staff to that of the children and young people so that an example of good practice can be established.

4. In the event of inappropriate use by adults, children and young people

Should a child or young person be found to misuse the on-line facilities whilst at school or in a setting the following consequences will occur:

- Any child found to be misusing the Internet by not following the Acceptable Use Rules will have a letter sent home to parents/carers explaining the reason for suspending the child's use for a particular lesson/activity.
- Further misuse of the rules will result in not being allowed to access the Internet for a period of time and another letter will be sent home to parents/carers.
- A letter will be sent to parents/carers outlining the breach in Child Protection Policy where a child is deemed to have misused technology against another child or adult.

In the event that a child or young person accidentally accesses inappropriate materials, the child will report this immediately to an adult and take appropriate action to hide the screen or close the window. Where a child feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkyouknow.co.uk) too make a report and seek further advice. The issue of a child or young person deliberately misusing online technologies should also be addressed by the establishment.

Children and young people should be taught and encouraged to consider the implications for misusing the Internet for example, posting inappropriate materials to websites via mobile phones etc, as this can lead to legal implications.

Guidance on the action taken for different scenarios is given as an appendix at the end of this document.

5. The Curriculum and tools for Learning
5.1 Internet Use

Google Chrome is used by staff and children in school. This search engine has built in security keeping staff and children secure. It has built in Malware and Phishing Protections with auto-updates to get the latest security fixes.

We teach our children and young people how to use the Internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding and communicating effectively in order to further learning, through Computing and/or PSHE lessons where the following concepts, skills and competencies have been taught by the time they leave Year 6:

- Internet Literacy
- Making good judgements about websites and e-mails received
- Knowledge of risks such as viruses and opening mail from strangers
- Access to resources that outline how to be safe and responsible when using any on-line technologies.
- File sharing and downloading illegal content
- Uploading information - know what is safe to upload and not upload personal information
- Where to go for advice and how to report abuse

These skills and competencies are taught within the curriculum so that children and young people have the security to explore how online technologies can be used effectively but in a safe and responsible manner. Children and young people will know how to deal with any incidents with confidence, as we adopt the 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have accidentally accessed something.

Personal Safety- ensuring information uploaded to websites and e-mailed to other people does not include any personal information including:

- Full name (first name is acceptable, without a photograph)
- Photograph of the child with any part of their name.
- Address
- Telephone number
- E-mail address
- School
- Clubs attended and where
- Age or DOB
- Names of parents
- Routes to and from school
- Think before you post a photograph, is it necessary? Does it identify other people? If so do I have their permission to post it? Lock it down so it cannot be copied.

Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that would also be acceptable in 'real life'. Parents/carers should monitor the content of photographs uploaded.

5.2 Social Media

Social networking is an excellent way to share news with family and friends. Providing the security of your profile had been set correctly and a strong password used, information should remain private. The danger is that few people understand profile privacy settings. The minimum age of use of a social networking site must be observed by a school, even though many pupils disregard this legal requirement.

Staff or adults need to ensure they consider the risks and consequences of anything they or their children and young people may post to any web or social networking sites, as inappropriate comments or images can reflect poorly on an individual and can affect future careers.

5.3 E-mail Use (Not currently applicable as children do not have their own school email addresses)

If and when children have email addresses to use as a class and as individuals as part of their entitlement to being able to understand different ways of communicating and using ICT to share and present information in different forms then:

Children may use the google drive to complete work set using their email addresses to send their work to a peer or to their teacher (school email) for peer assessment or marking. These emails are to be based around school work completed (no sensitive or confidential information to be sent).

Individual email accounts can be traced if there is an incident of misuse. Staff, children and young people are to use their school related email addresses for any communication between home and school only. A breach of this will be considered misuse and will result in consequences. Staff members must not give out and are not allowed to use their personal email address to contact children and young people under any circumstances. Parents/carers are encouraged to be involved with the monitoring of emails sent although the best approach with children and young people is to communicate about who they may be talking to and assess risks together. Teachers are expected to monitor their class use of emails where there are communications between home and school/setting on a regular basis.

5.4 Video and Photographs

The term 'image' refers to the taking of video footage or photographs via any camera or other technology. Personal photographs should not be uploaded that reveal more than a general location, an activity or a piece of work without express permission from parents/carers and school or setting. It is also recommended that permission is sought prior to any uploading of images to check for inappropriate content.

Particular care is required around the school website. Any photographs or video clips uploaded should not have a file name of a child. Photographs should only ever include the child's first name although Child Protection Guidance states either a child's name or a photograph but not both.

Group photographs are preferable to individual children and should not be of any compromising positions or in inappropriate clothing e.g. gym kit. A school trip is a common situation where photography by pupils and staff should be encouraged but there are potential dangers. The safest approach is to avoid the use of personal equipment and to use a school-provided item.

Care should be taken when storing photographs and ensure that these are stored appropriately. For instance to copy the photograph on to a personal laptop as opposed to school allocated laptop might make it difficult to retain control of how the picture is used. Memory cards, memory sticks and CD's should only provide a temporary storage medium. Once photographs are uploaded to the appropriate area of the school network, images should be erased immediately from their initial storage location.

It is important to continue to celebrate achievements of pupils through the appropriate use of photography in communicating with parents and the community.

6 Filtering and Safeguarding Measures

Anti- virus and anti-spyware software is used on all network and stand-alone laptops/Macs and is updated on a regular basis.

A corporate firewall ensures information about our children and young people and the school cannot be accessed by unauthorised users.

Children use a search engine that is appropriate such as Safesearch.

Links or feeds to e-safety websites are provided.

The Report Abuse button is available should there be concern of inappropriate or malicious contact made by someone unknown. This provides a safe place for children and young people to report and incident if they feel they cannot talk to a known adult.

7 Monitoring

Staff and children should be informed that monitoring is in place. The e-safety leader and/or a senior member or staff should be monitoring the use of on-line technologies by children and young people and staff on a regular basis. Network Managers should not have overall control; teachers should monitor the

use of the Internet during lessons and also monitor the use of emails between home and school on a regular basis.

Filtering or recording network usage will only be effective if monitored carefully to notice and report inappropriate access or usage. Often, this places a new responsibility on technical staff that they may not be trained for. This responsibility can become onerous if a pupil or staff member is apparently implicated in inappropriate or illegal activity.

It is wrong to assume that filtering and monitoring are simply technical ICT activities, solely managed by the network staff. Some technical staff have indeed taken on this wider responsibility to help ensure that ICT use is appropriate and beneficial. However, technical staff should not be expected to make judgements as to what is inappropriate material or behaviour, without support and supervision.

The monitoring policy must be set by the senior leadership team, with set procedures to deal with incidents. The senior leadership will require assistance from technical staff, but must also involve the school designated child protection co-ordinator and pastoral staff.

Linked Policies
Safeguarding & Child Protection
Behaviour Policy

APPENDICES

These are core statements or approaches which all settings are likely to want to adopt and adapt as appropriate.

- All users must take responsibility for their own use of new technologies, making sure that they use technology safely, responsibly and legally.
- All users must be active participants in e-safety education, taking personal responsibility for their awareness of the opportunities and risks posed by new technologies.
- No communications device, whether school provided or personally owned, may be used for the bullying or harassment of others in any form.
- All users have a responsibility to report any known misuses of technology, including the unacceptable behaviour of others.
- All users have a duty to respect the technical safeguards which are in place. Nay attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services, is unacceptable.
- All users have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
- All users have a duty to protect their passwords and personal network logins, and should log off the network when leaving workstations unattended. Any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
- All users should use network resources responsibly. Wasting staff effort or network resources, or using the resources in such a way as to diminish the service for other network users is unacceptable.
- All users should understand that network activity and online communications are monitored, including any personal and private communications made via the school network.

Staff Procedures Following Misuse by Staff
The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by an adult:

A. An inappropriate website is accessed inadvertently:
   - Report website to e-safety leader.
   - Contact the helpdesk so that it can be added to the banned or restricted list.
   - Change Local Control filters to restrict locally.
   - Check the filter level is at the appropriate level for staff use in our school.

B. An inappropriate website is accessed deliberately:
   - Ensure that no one else can access the material by shutting down.
   - Log the incident.
   - Report to Headteacher and e-safety leader immediately.
   - Headteacher to refer back to Acceptable Use Rules and follow agreed actions for discipline.

C. An adult receives inappropriate material:
   - Do not forward this material to anybody else – doing so could be an illegal activity.
   - Alert the Headteacher immediately.
   - Ensure the device is removed and log the nature of the material.
   - Contact relevant authorities for further advice i.e. police.

D. An adult has communicated with a child or used Computing equipment inappropriately with regard to children:
   - Ensure the child is reassured and remove them from the situation immediately, if necessary.

- Report to Headteacher and Designated Person for Child Protection immediately, who should then follow the Inter Agency Safeguarding Children Procedures.
- Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
- If considered innocent, refer to the Acceptable Use Rules for Staff and Headteacher to implement appropriate sanctions.
- If illegal or inappropriate misuse is known, contact Headteacher or Chair of Governors and Designated Person for Child Protection immediately and follow the Inter Agency Safeguarding Children Procedures.
- Contact CEOP (police) as necessary.

E. Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted:
   - This should be reported to the Headteacher.

Staff Procedures Following Misuse by Children and Young People:
The Headteacher will ensure that these procedures are followed, in the event of any misuse on the Internet, by a child or young person.

A. An inappropriate website is accessed inadvertently:
   - Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.
   - Report website to the e-safety leader if this is deemed necessary.
   - Contact the helpdesk so that it can be added to the banned list or use Local Control to alter within your settings.
   - Check filter level is at the appropriate level for pupil use in school.

B. An inappropriate website is accessed deliberately:
   - Refer the child to the Acceptable Use Rules that were agreed.
   - Reinforce the knowledge that it is illegal to access certain images and police can be informed.
   - Decide on appropriate sanction.
   - Notify the parent/carer.
   - Inform LA as above regarding filtering.

C. An adult or child has communicated with a child or used ICT equipment inappropriately:
   - Ensure the child is reassured and remove them from the situation immediately.
   - Report to the Headteacher and Designated Person for Child Protection immediately.
   - Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
   - If illegal or inappropriate misuse i.e. where it appears that the incident refers to grooming or child exploitation the Headteacher must follow the Inter Agency Safeguarding Children Procedures.
   - Contact the safer schools officer and local Police as necessary.

N.B. There are three incidences when you must report directly to the police as well as the Headteacher and e-safety leader.
- **Indecent images of children found.**
- **Incidents of 'grooming' behaviour.**
- **The sending of obscene materials to a child.**

It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.

Acceptable Use Rules for Staff
These rules apply to all on-line use and to anything that may be downloaded or printed.
Adults must abide by these Acceptable Use Rules so that they provide an example to children and young people for the safe and responsible use of on-line technologies which will educate, inform and protect so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal email and should use the school email address upon agreed use within the school.
- I know that I should only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children and young people before they can upload images (videos or photographs) to the Internet or send them via email.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the Internet.
- I will report any accidental misuse.
- I will report any incidents of concern for the children's safety to the Headteacher, Designated Person for Child Protection or the e-safety leader in accordance with procedures listed in this policy.
- I know who my Designated Person for Child Protection is.
- I know that I should not be using the school system for personal use unless this has been agreed by the Headteacher/ E-safety leader.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will only install hardware and software I have been given permission for.
- I will ensure that I follow The Data Protection Act 1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and do not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requires my password I will check with the e-safety leader.
- I understand the Acceptable Use Policy and the procedures that I should follow.

Links to other policies

Child Protection & Safeguarding

Anti-bullying