OUR LADY OF PITY R.C. PRIMARY SCHOOL

DO EVERYTHING WITH LOVE

Our Lady of Pity R.C. Primary School

E-Safety Policy

Reviewed by Governing Body: November 2022

Introduction and Rationale

This policy has been written to:

- Set out the key principles expected of all members of the school community at Our Lady of Pity R.C. Primary School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Our Lady of Pity.
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use. (see appendices)
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Help parents understand how they can help their child stay safe online.

At Our Lady of Pity, we wish to make use of ICT hardware and software to enhance children's learning opportunities and understanding. We seek to use such devices to share information, communicate and connect electronically to the wider world in a safe, controlled manner. Staff will make use of systems such as email and online calendars to assist in the smooth day-to-day running of the school. We wish to allow children to use ICT safely and responsibly and educate them in the benefits and potential dangers of ICT and ensure children know how and why it is important to protect themselves online.

For the purpose of this document, e-safety may be described as the school's ability:

- to protect and educate pupils and staff in their use of technology
- to have the appropriate mechanisms to intervene and support any incident where appropriate.

The breadth of issues classified within e-safety is considerable, but can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material
- contact: being subjected to harmful online interaction with other users
- conduct: personal online behaviour that increases the likelihood of, or causes, harm.

This policy will be shared with Governors, staff and parents via the school website. It will be reviewed and updated regularly and as need arises, for example with the introduction of new technology, social medias, apps, devices etc

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Roles and responsibilities

The Local Governing Board

The local governing board has overall responsibility for monitoring this policy and holding the Head of School to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (see appendices)

The Head of School

The Head of School is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead(s)

Details of the school's DSLs are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Head of School in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head of School, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head of School and/or governing board

This list is not intended to be exhaustive.

The ICT Provider

The ICT provider is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (see appendices), and ensuring that pupils follow the school's terms on acceptable use (see appendices)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff or the Head of School of any concerns or queries regarding this policy
- Ensure they and their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (see appendices)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (see appendices).

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*

- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*
- *How information and data is shared and used online*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

The safe use of social media and the internet will also be covered in other subjects where relevant.

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website, newsletters and through parent workshops.

This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head of School and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Head of School.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.
Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to follow an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements (see appendices).

Mobile Phones

- Expectations of staff and mobile phones are set out in the IT User Agreement.
- Children are not permitted to use mobile phones in school. This is covered in the IT User Agreement
- Mobile phones may be brought into school, but must be switched off, and handed in to the school office at the start of the day.
- Phones are stored in a locked cabinet.
- Phones will be handed back to pupils at the end of the day (3.25pm)
- The school is not responsible for any loss or damage to any phone brought in.

Photographs and videos

- Guidance relating to staff taking photos and videos of children is set out in the IT User Agreement (ICT)

- Parents give consent when they start school in F2 and then are reminded to review annually.
- The permissions form grants the school and Trust permission to take photographs/videos of their child for the use of: assessment, displays, artwork, publicity materials etc
- The slip outlines where the photographs/videos may be made public i.e. on the school website, Twitter account, displays around the school, prospectus, press material etc
- Where a photograph is used in public, the child's full name will not be included

- Parents have the right to request that no images/videos of their child are taken. In such cases, the school will do all it can to ensure that this wish is followed in a sensitive manner in order that the child does not feel 'left out'. However, the Head of School will explain to the parents that while the school will not take images and will take all steps it can to ensure that images are not taken by others, there are implications for guaranteeing such a request, so that the child does not appear in the background of any pictures. Such implications may include – the child not participating in events where photographs are likely to be taken such as sports days, concerts and plays etc
- Any photographs or videos of children will only be taken by staff on school equipment, not personal cameras, mobile phones or tablets. The only exception to this are the members of staff who upload to social media accounts/website. This allows photographs to be taken and uploaded quickly and easily. Where a photograph is taken, the Head of School will be told and shown the image. The images will be deleted after upload.
- Photographs/videos of children will be stored securely on the school Google Drive. Images will not be kept for long periods of time unnecessarily i.e. once the child has left the school and there is no justifiable reason for them to be kept

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the school office in the first instance.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our Behaviour Policy and IT and Internet Acceptable Use Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Disciplinary Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety using CPOMS

This policy will be reviewed every 2 years by the Head of School. At every review, the policy will be shared with the governing board.

Other policies referenced

IT Acceptable Use Agreement

All staff (including Governors, volunteers, supply etc.) who work at Our Lady of Pity RC Primary School have read and agreed to the IT Acceptable Use Agreement. The agreement covers various aspects of e safety including

- Use of personal Social Media Accounts
- Mention of the school, pupils or staff in any electronic form
- Responsible and professional use of the school e mail system
- Appropriate use of all ICT devices including mobile phones during the school day/on site

Social Media Policy (see appendices)

A separate policy relating to school social media accounts has been written. A summary of key points:

- The Administrator will be responsible for monitoring the account and blocking any inappropriate followers (pupils are counted as 'inappropriate followers' due to the Twitter age restriction of 13)
- The account will be used for sharing school information e.g. Parents Evening dates and for celebrating pupils' achievements e.g. a photograph of art work
- The account will not be a discussion forum and the account will not reply to any 'replies' from followers

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1 - E–SAFETY AGREEMENT FOR STAFF

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.

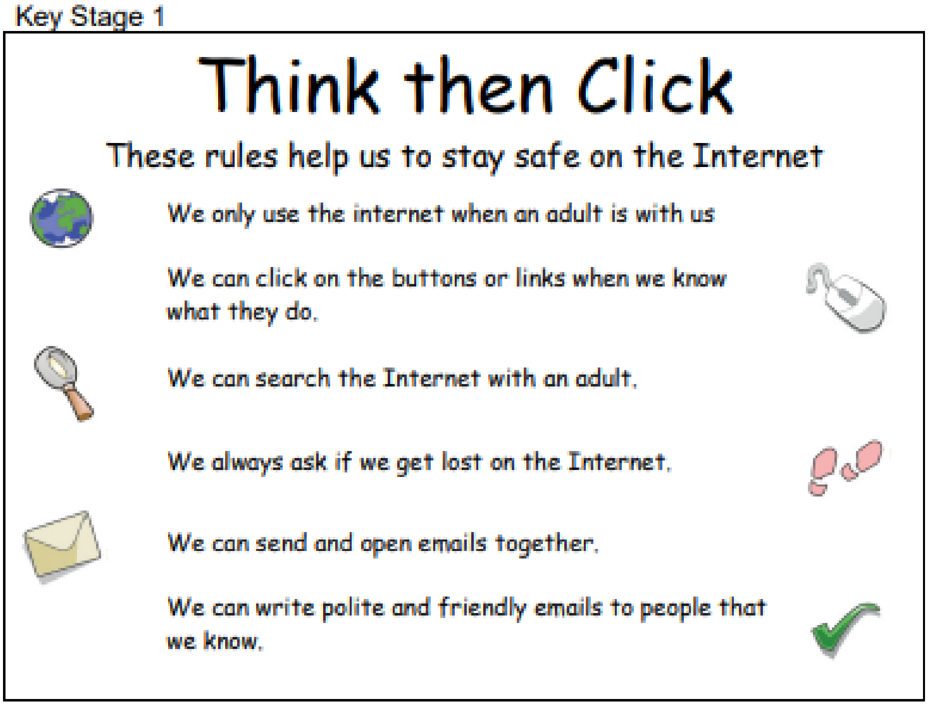
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner. This school expects that all activity should be related to a professional use.
- I appreciate that ICT includes a wide range of systems, including mobile phones, tablet computers, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business. It is my responsibility to ensure that I do not store any inappropriate material on these devices in school.
- I understand that school information systems may not be used for private purposes without specific permission from the Head of School.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance. This is managed by Mercu.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Head of School and/or the Designated Safeguarding Lead(s).
- I will ensure that electronic communications with pupils and parents including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote digital safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I am aware that I cannot use personal devices or mobile networks to access inappropriate content at school. The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
- I have read, understood and accept the Staff Code of Conduct for ICT.

SIGNED:

DATE:

Appendix 2 - E-SAFETY AGREEMENT FOR PUPILS

Key Stage 1



Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

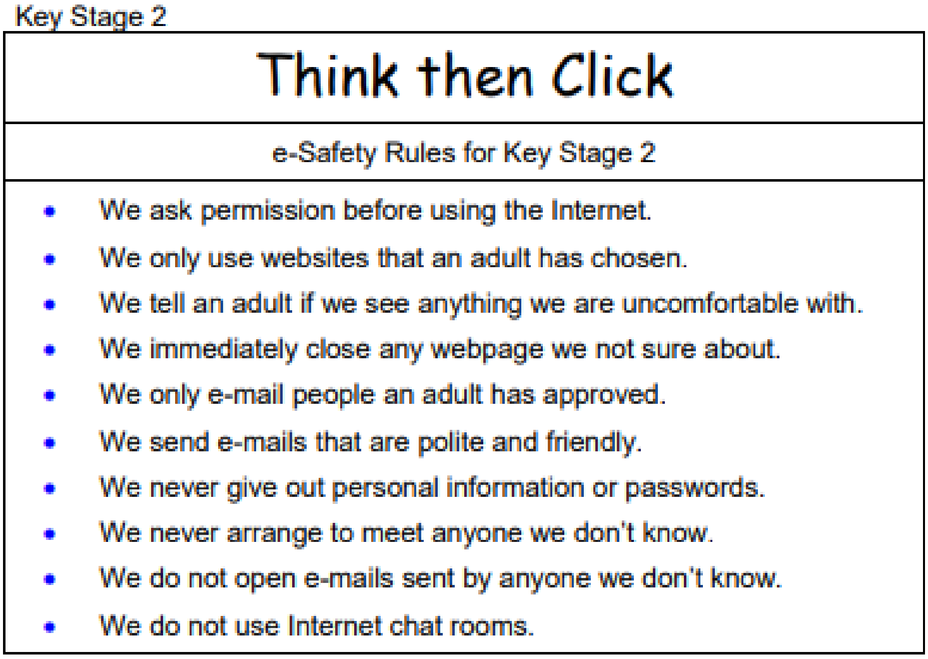
We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Key Stage 2



Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

Appendix 3 - PERMISSIONS FOR INTERNET/NETWORK USE

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-safety rules have been understood and agreed.

Our e-safety policy is published on the school's website.

Pupil: Year Group:

Pupil's Agreement

- I have read and I understand the school e-safety rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed: Date:

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my child to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: Date:

Please print name:

Please complete, sign and return to the School Office

Appendix 4 - E-SAFETY AGREEMENT FOR VISITORS

Consent Form for Visiting Adults Using our Network and Internet Access

All adults have to be responsible when using information systems. As visitors to schools, adults have to be aware that their activities must be related to education or their role within the school (PTA administration, family learning etc). Any abuse of this privilege could result in access being removed. In cases where the school feels that either their pupils or staff have been placed at risk, this could lead to the incident being reported to the police.

All visitors should consult the school's e-safety policy for further information and clarification. This is available through the school office or the school's website.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner. This school expects that all activity should be related to a professional and educational use.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business. It is my responsibility to ensure that I do not store any inappropriate material on these devices in school.
- I understand that school information systems may not be used for private purposes without specific permission from the Head of School.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that no files are removed from the school's network without the express permission of a senior member of the school's staff.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Head of School.
- I will ensure that all e-mail communication is appropriate.
- I will not access any inappropriate websites including social networking sites.
- I am aware that I cannot use personal devices or mobile networks to access inappropriate content at school.

I have read, understood and accept the Visitor's Code of Conduct for ICT

SIGNED:	DATE:

Appendix 5 - MOBILE PHONE POLICY

This policy applies to all individuals who have access to personal or work-related mobile phones on site. This includes staff, volunteers, children, young people, parents/ carers, visitors and community users.

Introduction

Mobile phone technology has advanced significantly over the last few years - and it continues to evolve. Wireless connections in particular have extended the capabilities of mobile phones, enabling access to a wide range of new content and services globally. Many phones now offer Internet and email access, alongside the most often standard functions of messaging, camera, video and sound recording. Mobile phones, alongside other forms of technology are changing the way and speed in which we communicate. They can provide security and reassurance. However, there are also associated risks. Children and young people need to understand these risks in order to help them develop appropriate strategies for keeping themselves safe. As with e-safety issues generally, risks to children and young people can be broadly categorised under the headings of content, contact and conduct and managed by reducing availability, restricting access and increasing resilience.

Aim

The aim of the Mobile Phone Policy is to promote safe and appropriate practice through establishing clear and robust acceptable use guidelines for staff, visitors and children. This is achieved through balancing protection against potential misuse with the recognition that mobile phones are effective communication tools - which in turn can contribute to safeguarding practice and protection.

Policy

It is recognised that it is the enhanced functions of many mobile phones that cause the most concern, and which are most susceptible to misuse. Misuse includes:

- taking and distribution of indecent images
- exploitation and exposure to emotional harm through being exposed to inappropriate content
- bullying through sharing content, images or videos.

It is also recognised that mobile phones can cause an unnecessary distraction during the working day and can be intrusive when used in the company of others. When mobiles phones are misused it can impact an individual's dignity, privacy and right to confidentiality. Such concerns are not exclusive to children and young people; hence there is a duty to protect the needs and vulnerabilities of adults and visitors.

School's Expectations

Staff:

- Staff must only use mobile phones for personal use in office areas or staff room.
- Mobile phones must only be on outside school hours and during lunch break. The only exception to this is senior, pastoral and site staff who are on call for work purposes. This includes:

    - Executive Headteacher
    - Head of School
    - Caretaker
    - IT Technician
- Staff using mobile phones for work must avoid unnecessary use in the vicinity of children. An example of this could be the caretaker, site manager or a senior member of staff being contacted.
- Staff must not take images of children or store any data relating to children on their mobile phones.
- Staff, volunteers and trainee teachers are not permitted to use their own personal phones for contacting children, young people and their families within or outside of the setting unless authorised by a member of the SLT.
- Staff should not access content that is not suitable for professional use during working hours whilst on school site. This includes social networking, pornography, inappropriate websites, dating websites etc.
- During school trips staff must only use phones for business reasons around children. They may need to be turned on for emergency contact needs.
- During residential trips staff will use mobile phones to contact families but must do this is an area away from children. Privacy of room, quiet space etc.
- Personal calls are not permitted to be made on a work mobile, other than in agreed exceptional circumstances. On residential strips, staff would do this as part of a designated break.
- If any practitioner is required to drive in a working capacity, and has responsibility for a work mobile, the phone must be switched off whilst driving. It is strongly recommended that practitioners follow the same procedures regarding their own personal mobile phones. Under no circumstances should practitioners drive whilst taking a phone call. This also applies to hands-free and wireless connections, which are considered a distraction rather than a safer alternative.
- Staff should ensure that their mobile phones are locked away safely if in school. They can be left at the office for safe storage. To protect themselves, staff should have their phone password protected.
- As well as safeguarding children and avoiding any unnecessary disruptions during the day, this procedure also aims to protect staff against any unfounded allegations.
- Staff who need to be available for emergency contact should give the school's phone number for contact during working hours. All phones are manned during the working day between 8.45-4.30pm. After this staff not supervising children may need to have their phones switched onto vibrate for emergency contact.

This will be covered in induction. Staff who don't follow this code may be subject to disciplinary action.

Visitors:

- Parents/Visitors cannot use mobile phones on premises.
- Photographs can only be taken at authorised events such as carol concerts, performances etc. Parents have signed consent forms accepting their responsibility to use any images for personal use and not to share on any social networking sites.

- Other professionals must not use mobile phones in the immediate vicinity of children. We recognise that contractors, IT technicians will need access to mobile phones. They will be directed to office or staffroom areas.
- Professionals making or receiving work calls must do so in the office or staff room areas.
- Visitors should not access content that is not suitable for professional use whilst on school site. This includes social networking, pornography, inappropriate websites, dating websites etc.
- During school trips, volunteers must have mobile phones switched off.

Visitors who don't follow this code may be asked to leave the premises. They may not be allowed to return.

Children:

- Children are never allowed to use mobile phones on school site.
- Children may bring phones into school in years 6 but must follow the following protocol:
  - Phones must be turned off before the enter the premises
  - Phones must be handed into the school office. Phones remain there until the end of the school day.
  - Phones should be collected at the end of the day and put in their bag/pocket.
  - Phones cannot be turned on until children leave the premises.

- Under no circumstances is any child permitted to take images or make recordings on a mobile phone.
- Children cannot bring phones on school trip or residential visits.
- Children not following these safety guidelines will:
  - Have their phone removed and placed at the school office. It must be collected by an adult from here.
  - If a second offence occurs in the calendar year, they will have their phones removed and left with a senior member of staff. They will also lose the privilege of being allowed a mobile phone for an agreed length of time between the school and parent.

Appendix 6 - SOCIAL MEDIA POLICY

1. POLICY STATEMENT

1.1 The internet and use of apps provides opportunities to participate in interactive discussions and the sharing of information using a wide variety of social media such as Facebook, Twitter, Instagram, blogs and wikis. However, employees' use of social media can pose risk to the School's confidential and proprietary information, and reputation.

1.2 To minimise these risks and to ensure that the School's IT resources and communications systems are used only for appropriate purposes, the School expects employees to adhere to this policy. Policy will be reviewed every two years and shared with staff.

1.3 This policy does not form part of any employee's contract of employment and it may be amended at any time.

2. WHO IS COVERED BY THIS POLICY?

2.1 This policy covers all individuals working at all levels throughout the School, including part time and fixed term employees, casual staff, agency staff and volunteers (collectively referred to as staff in this policy).

2.2 Third parties who have access to the School's electronic communication systems and equipment are also required to comply with policy.

3. SCOPE AND PURPOSE OF THE POLICY

3.1 This policy deals with the use of all forms of social media, including Facebook, Instagram, Twitter, Wikipedia, all other social networking sites, and all other internet postings, including blogs.

3.2 It applies to the use of social media for both professional and personal purposes, whether during work hours or otherwise. The policy applies regardless of whether the social media is accessed using the School's IT facilities and equipment or equipment belonging to members of staff.

3.3 Breach of this policy may result in disciplinary action up to and including dismissal.

3.4 Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether the School's equipment or facilities are used for the purpose of committing the breach.

3.5 Any member of staff suspected of committing a breach of this policy will be required to co-operate with any investigation that may follow, which may involve handing over relevant passwords and login details for school provided hardware, software and remote access.

3.6 Staff will be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

4. PERSONNEL RESPONSIBLE FOR IMPLEMENTATION OF THE POLICY

4.1 The Board of Governors has overall responsibility for the effective operation of this policy, but has delegated day-to-day responsibility for its operation to the Head of School. Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks also lies with the Head of School.

4.2 All managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements. Training will, if required, be provided to facilitate this.

4.3 All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to the Head of School.

4.4 Questions regarding the content or application of this policy should be directed to the Head of School.

5. COMPLIANCE WITH RELATED POLICIES AND AGREEMENTS

5.1 Social media should never be used in a way that breaches any the other policies of the School. If an internet post would breach any of the School's policies in another forum, it will also breach them in an online forum. Staff are prohibited from using social media to:

5.1.1 breach any obligations the school has in relation to the duty of confidentiality to its staff and pupils, both past and present;

5.1.2 breach our disciplinary policy;

5.1.3 defame or disparage the School its staff, pupils and third parties connected with the school, for example pupils' parents;

5.1.4 breach the school's anti-harassment and bullying policy;

5.1.5 breach the school's equal opportunities policy;

5.1.6 breach the data protection policy;

5.1.7 breach any other laws or ethical standard (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements).

5.2 Staff should never provide references for other individuals on social or professional networking sites. Such references, whether positive or negative, can be attributed to the School and create legal liability for the School accordingly and the individual providing the reference.

5.3 Employees who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

5.4 If we have authorised use using apps such as twitter, see-saw etc staff will be sharing good news on behalf of the school. If any inappropriate content is posted they should report that to the provider (Twitter etc) and to the head teacher. They do not need to comment themselves.

5.5 Staff may support PTA groups on social media but should not comment on school business, other staff or children.

6. PERSONAL USE OF SOCIAL MEDIA Personal use of social media is never permitted during working time or by means of the School's computers, networks and other IT resources and communications systems.

7. MONITORING

   7.1 In light of the exemption of personal use of social media during working time, the contents of the School's IT resources and communications systems are the School's property. Staff should therefore have no expectation of privacy in any messages, files, data, document or social media post conversation or message transmitted to, received or printed from, or stored or recorded on the School's electronic information and communications systems.

   7.2 The Board of Governors of the School reserve the right to monitor, intercept and review, without further notice, staff activities using the School's IT and communication systems, including but not limited to social media postings and activities to ensure that rules are being complied with, and for legitimate business purposes. You consent to such monitoring by your use of such resources and systems.

   7.3 Staff should not use the School's IT resources and communications systems for any matter that he/she wishes to be kept private or confidential.

8. BUSINESS USE OF SOCIAL MEDIA

   8.1 It is unlikely that any member of staff will be required to speak on behalf of the School in a social media environment, but in the event that you are, you must still seek the approval for such communication from the Head Teacher who may require you to undergo training before you do so and impose certain requirements and restrictions with regard to your activities.

   8.2 Likewise, if you are contacted for comments about the School for publication anywhere, including in any social media outlet, you should direct the enquiry to the Head Teacher and do not respond without written approval.
   8.3 The use of social media for business is subject to the remainder of this policy.

9. RECRUITMENT We may use internet searches to perform due diligence on candidates in the course of recruitment. Where the School does this, it will act in accordance with its data protection and equal opportunities obligations.

10. RESPONSIBLE USE OF SOCIAL MEDIA

    10.1 Staff have to accept that their professional responsibilities trump that of their personal considerations. Staff should not have friends/link on social media who are parents at the school. This ensures that there is no abuse of privacy either directly or indirectly (friends of friends links etc).

    10.2 Staff must not have social media links with ex-pupils until they are over aged 21. This prevents abuse of power situations with minors.

10.3 The following sections of the policy provide staff with common-sense guidelines and recommendations for using social media responsibly and safely.

10.4 Protecting the School's reputation:

10.4.1 Staff must not post disparaging or defamatory statement about:

10.4.1.1 the School as an organisation;

10.4.1.2 members of staff or pupils;

10.4.1.3 third parties connected with the School, e.g. parents

10.5 Staff should also avoid social media communications that might be misconstrued in a way that could damage the School's reputation.

10.6 Staff should make it clear in social media postings that they are speaking on their own behalf, and not on behalf of the School or The Board of Governors A way to achieve this would be writing in the "first person".

10.7 If you disclose your affiliation with the School you should state that your views do not represent those of your employer. For example, you could state, "the views in this posting do not represent the views of my employer".

10.8 Staff are personally responsible for what they communicate in social media.

10.9 Staff should ensure that the content of their postings is consistent with professional image as an employee of the School.

10.10 If you are uncertain or concerned about the appropriateness of any statement or posting, you should refrain from making the communication until you discuss it with the Head Teacher.

10.11 If you see content in social media that disparages or reflects poorly on the School or any member of staff, you should contact the Head Teacher on behalf of the Board of Governors.

10.12 Staff should not do anything to jeopardise confidential information of the School, its staff or pupils through use of social media.

10.13 Staff should avoid misappropriating or infringing the intellectual property of other companies and individuals as this may create liability for the School and the individual concerned.

10.14 Staff should not post anything that colleagues would find offensive, including discriminatory comments, insults or obscenity.

10.15 Staff should not post anything related to your colleagues or pupils without their or their parents' written permission and consent.