Holy Spirit Catholic Primary School

E-Safety Policy

This policy was approved by	Governors
Name	
Position	Governors
Date	Sept 2021
Review Date	Sept 2022

Mission Statement

Our school is a place where we respect the views and value the opinions of everyone.

We encourage the development of behaviour and attitudes which reflect the life of Christ and the teachings of the gospel and so nurture the appreciation of every individual regardless of race, gender, colour or creed.

We endeavour to involve teachers, parents, governors and the wider community in the spiritual, intellectual, emotional and social development of our children.

We strive to help our young people become more independent, making their own decisions and taking responsibility for themselves and others.

“Jesus holds my hand and guides me on my way”

E-Safety Policy – May 2021 (Review May 2023)

The e-Safety Policy relates to other policies including the Acceptable Use Policy, ICT Policy, the Cyberbullying Policy and the policy for Child Protection. The school e-Safety Coordinator is Laura Kelly. This e-Safety Policy has been written by the school and has been approved by Governors.

Whilst care has been taken to consider all aspects of E Safety there may be times when members of staff, schools and services need to make independent judgments on individual situations not covered in this document. It is expected that in these circumstances that all staff will advise their senior colleagues of such action taken or proposed and schools will seek further advice from HR.

This document applies to all members of staff employed either directly or indirectly by Holy Spirit Catholic Primary School. All members of staff are expected to adhere to this code of practice to ensure the safety of the young people in their care and in doing so fully abide by the guidance contained herein. Any member of staff found to be in breach of these guidelines may be subject to disciplinary action.

For the purpose of this document 'Students', 'Pupils', 'Children' and 'Young People' will refer to all children and young people who members of staff have contact with as part of their professional capacity and to which all staff have a professional duty of care.

For the purpose of this document 'Schools', 'Services' and 'Organisations' will refer to the employer and place of work of all members of staff, whether the place of work is permanent, temporary or peripatetic.

Aim

The aim of this policy is to inform all staff of best practice around E-Safety and draw attention to existing local and national guidance on this subject. It is our responsibility to safeguard young people and protect staff from false accusations of improper conduct so that together we can ultimately maintain the safest possible learning and working environments for children and staff alike.

Teaching and learning

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum, a necessary tool for staff and pupils and will enhance learning. The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. *(Please refer to the Acceptable Use Policy.)*

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will also be taught how to evaluate Internet content and should be taught to be critically aware of the materials they read. All pupils will be shown how to validate information before accepting its accuracy. Purple Mash will be followed to ensure effective progression and coverage to enable these skills, knowledge and understanding to be developed throughout all three key stages.

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Equipment on loan to a member of staff (e.g., laptop) should be used solely by the member of staff; it is not acceptable to loan the equipment to someone else.

Social Contact with Pupils, Children or Young People

Staff must not establish or seek to establish social contact with pupils, children or young people for the purpose of securing a friendship or to pursue or strengthen a relationship. Even if a pupil, child or young person seeks to establish social contact, or if this occurs coincidentally, the member of staff should exercise his or her professional judgement in making a response and be aware that such social contact could be misconstrued.

All contact with pupils, children or young people should be through appropriate channels at all times. Any communication outside of agreed professional boundaries could be prone to misinterpretation and as a result could put both the employee and young person at risk.

Staff should not give, nor be required to give, their personal details such as home or mobile phone number, Instant Messenger identities or personal e-mail address to pupils, children or young people. Staff should not use any of the above means to contact pupils, children or young people without the prior and explicit consent of Senior Leadership. Any member of staff found to be in contact with pupils, children or young people through any of the above means, or any other unapproved method, without prior consent could be subject to disciplinary action.

Internal e-mail and approved contact systems should only be used in accordance with the appropriate school or service Information Security Policy.

Members of staff should:

- Always seek approval from senior leadership for any planned social contact with pupils, children or young people for example when it is part of a reward scheme or pastoral care programme
- Advise senior leadership of any regular social contact they have with a pupil, child or young person which may give rise to concern
- Report and record any situation which they feel might compromise the reputation of the organisation or their own professional standing

Internet Use

Members of staff must follow and adhere to the policies on the use of IT equipment at all times and must not share logins or password information with other members of staff, pupils, children or young people, friends, family or members of the public.

Under no circumstances should members of staff in the workplace access inappropriate images using either personal or work-based equipment. Accessing child pornography or indecent images of children on the internet, and making, storing or disseminating such material is illegal and if proven will invariably lead to disciplinary action the individual being barred from work with children and young people.

Using work-based equipment to access inappropriate or indecent material, including adult pornography, either in the workplace or at home, will give cause for concern particularly if as a result children or young people might be exposed to inappropriate or indecent material and may also lead to disciplinary action.

Managing Internet Access

Information system security

The School's ICT systems capacity and security will be reviewed regularly, and virus protection will be updated regularly.

E-mail

- Pupils may only use approved e-mail accounts on the school system (if agreed as part of study)
- Pupils must immediately tell a teacher if they receive offensive e-mail
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- The forwarding of chain letters is not permitted

(Please refer to 'Think and Click' Internet Safety rules displayed and the Acceptable Use Policy.)

Published content and the school web site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. The headteacher and head of school/deputy head will take overall editorial responsibility and ensure that content is accurate and appropriate.
Photographs of pupils and pupils' full names will not be used anywhere on the Web site or Blogs.

Social networking and personal publishing

Members of staff must not have any contact with pupils, children or young people through such sites and staff must not add pupils, children or young people as friends or respond to requests for friendship from children if asked. If a member of staff suspects that an existing friend is a student, child or young person, they should take reasonable steps to check the identity of the individual and end the friendship should the suspicions not be put to rest.

It is recognised that personal access to Social Networking sites outside the work environment is at the discretion of the individual. However, members of staff should consider their use of social networks as they take on the responsibilities of a professional, taking particular care to secure personal information and ensure their use of such networking sites is respectable and appropriate at all times.

Personal profiles on social networking sites and other internet posting forums must not identify your employer or place of work and careful consideration should be given to information which is published on such sites. For example, information which is confidential or could put others at risk should not be posted on such public domains. If the material you post or display is considered inappropriate or could be considered to bring your school or profession into disrepute, disciplinary action may be considered.

Schools ICT service providers will block/filter access to social networking sites. Pupils will be advised never to give out personal details of any kind which may identify them or their location. (Please refer to 'Think and Click' Internet Safety rules displayed in all classrooms and the Acceptable Use Policy). Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Inappropriate Material

When considering what is defined as inappropriate material it is important to differentiate between inappropriate and illegal and inappropriate but legal. All staff should be aware that in the former, case investigation may lead to criminal investigation, prosecution dismissal and barring. In the latter it can still lead to disciplinary action, dismissal and barring even if there is no criminal prosecution.

It is illegal to possess or distribute indecent images of a person under 18 and viewing such images on-line may constitute possession even if not saved. Accessing child pornography or indecent images of children on the internet, and making, storing or disseminating such material is illegal and if proven will invariably lead to the individual being barred from work with children and young people.

Material which incites hate, harm or harassment

There are a range of offences in relation to incitement of hatred on the basis of race, religion, sexual orientation and particular offences concerning harassing or threatening individuals which includes cyber bullying by mobile phone and social networking sites etc. It is an offence to send indecent, offensive or threatening messages with the purpose of causing the recipient distress or anxiety.

Professionally Inappropriate Material

Actions outside the workplace that could be considered so serious as to fundamentally breach the trust and confidence in the employee may constitute Gross Misconduct. These actions may not always be illegal. For example, using work equipment to access inappropriate or indecent material, including 'adult pornography', will give the school or service rightful cause for concern particularly if as a result children or young people might be exposed to inappropriate of indecent material. Such behaviour would be considered inappropriate and could result in disciplinary action.

Some examples of inappropriate material and actions are:

- Posting offensive or insulting comments about colleagues on social networking sites.
- Accessing adult pornography on work-based computers during break.
- Making derogatory comments about pupils or colleagues on social networking sites.
- Posting unprofessional comments about one's profession or workplace on social networking sites.
- Making inappropriate statements or asking inappropriate questions about pupils on social networking sites
- Contacting pupils by email or social networking without senior staff approval.
- Trading in fetish equipment or adult pornography.

Managing filtering

The school will work with the service providers to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator or member of the Senior Leadership Team.

Creating Images of pupils through Photography and Video

Many work-based activities involve recording images, and these may be undertaken as part of the curriculum, extra school activities, for publicity, or to celebrate achievement. However, written permission should be gained from legal guardians as well as senior management prior to creating any images of children.

Using images of children for publicity purposes requires the age-appropriate consent of the individual concerned and their legal guardians. Images will not be displayed on the school website, in publications or in a public place without such consent. The definition of a public place includes areas where visitors to the school or service provision have access.

Photograph or video images where possible must be created using equipment provided by the workplace. However, it is acceptable to record images of children on personal equipment such as personal cameras, mobile phones or video cameras for the use on the school website or the school twitter account. These images must then be deleted without being stored for personal use.(Ideally witnessed by a member of senior staff.)

Members of staff creating or storing images of children using personal equipment without prior consent may be subject to disciplinary action. For convenience, staff might use their own mobile phones to take a photograph or video; once used, this must be deleted (no images should be stored longer than necessary; if an image is needed for more than 24 hours, school equipment or school-approved equipment might be used).

Members of staff must:

- be clear about the purpose of the activity and about what will happen to the photographs when the lesson/activity is concluded
- ensure that senior management is aware that photography/image equipment is being used and for what purpose
- ensure that all images are available for scrutiny in order to screen for acceptability
- be able to justify images of children in their possession
- avoid making images in one-to-one situations

Members of staff must not take, display or distribute images of children unless they have consent to do so. Failure to follow any part of this code of practice could result in disciplinary action being taken.

Managing videoconferencing

Video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet. Pupils should ask permission from the supervising teacher before making or answering a videoconference call. Videoconferencing will be appropriately supervised for the pupils' age.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Use of personal technology/equipment in school

The use of any personal equipment in schools should always be with the prior permission of senior management in order to comply with health and safety regulations and members of staff should take care to comply with acceptable use and IT policies.

Personal equipment capable of recording images, moving images or sounds and those used for accessing the internet such as iPads, mobile phones, cameras, video cameras and laptops should not be used in work time without the prior permission of senior management.

Any member of staff found to be using such personal equipment without prior authorisation may be subject to disciplinary action.

Propriety and Behaviour

All members of staff have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of children and young people. They should adopt high standards of personal conduct in order to maintain the confidence and respect of their peers, children and the public in general.

Members of staff should not behave in a manner which would lead any reasonable person to question their suitability to work with children or act as a role model. This includes behaviour in virtual online communities' as well day to day social situations. Members of Staff also should not make (or encourage others to make) unprofessional personal comments through online media which scapegoat demean or humiliate or might be interpreted as such.

An individual's behaviour, either in or out of the workplace, should not compromise his or her position within the work setting nor bring the school or organisation into disrepute.

If an allegation is received that a member of staff is responsible for comments made (online or otherwise) which could be deemed harmful, threatening, defamatory or abusive to the school or organisation, this will be investigated using the appropriate procedure. Any actions which bring the organisation or profession into disrepute will be considered under the appropriate policy and appropriate action taken in line with that procedure.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Confidentiality

Members of staff may have access to confidential information about pupils, children or young people and the organisation in order to undertake their everyday responsibilities and in some circumstances, this may be highly sensitive or private information. Such information should never be shared with anyone outside the school, a member of the public or outside agencies, except in specific circumstances, for example when abuse is alleged or suspected. In such cases, individuals have a duty to pass information on without delay, but only to those with designated child protection responsibilities or a senior member of staff.

Care should be taken with the storage of such confidential information. Confidential information should never be stored on personal computers or devices or distributed through personal email or internet channels. Only authorised school-based devices and systems should be used to store and transfer confidential information. Members of Staff found to be compromising confidentiality by use of unauthorised systems and devices could be subject to disciplinary action.

Authorising Internet access

The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up to date, for instance a member of staff may leave, or a pupil’s access be withdrawn. Pupils will be supervised at all times. All parents/carers will be asked to sign and return a consent form.

Cyberbullying (Refer to the Anti bullying Policy)

All forms of bullying, including cyberbullying, are taken very seriously. Bullying is never tolerated, and it is not acceptable for any member of staff to behave in a manner which is intimidating, threatening or in any way discriminatory. Behaviour which constitutes Bullying or Harassment may be dealt with under the Anti-Bullying Policy and could result in disciplinary action.

However, this doesn’t only extend to behaviour within the workplace. In some instances, bullying or harassment that occurs outside the workplace where there is a link to employment could also fall under the responsibility of the employer and therefore result in disciplinary action being taken against the responsible individual.

Certain activities relating to cyberbullying could be considered criminal offences under a range of different laws. Cyberbullying consists of threats, harassment, embarrassment, humiliation, defamation or impersonation and could take the form of general insults, prejudice-based bullying or discrimination through a variety of media. Media used could include email, Virtual Learning Environments, chat rooms, web sites, social networking sites, mobile and fixed-point phones, digital cameras, games and virtual world sites.

If an allegation is received that a member of staff is responsible for comments made online which could be deemed harmful, threatening, defamatory, abusive or harassing in any way towards another employee, the organisation will investigate this matter. Any allegation of Bullying or Harassment made by an employee against another member of staff where the accused uses the internet, mobile phone, text message or email, along with any other forms of abuse, may be dealt with through the Bullying and Harassment policy and could lead to disciplinary action.

Staff is required to take steps to protect themselves and their personal information by:

- Keeping all passwords secret and protect access to their online accounts
- Not befriending children and young people on social networking services and sites
- Keeping personal phone numbers private
- Not using personal phones to contact parents and pupils, children and young people (if necessary then block number)
- Keeping personal phones secure, i.e. through use of a pin code, when within work
- Not posting information about themselves that they wouldn't want employers, colleagues, pupils, children, young people or parents to see
- Not retaliating to any incident
- Keeping evidence of any incident
- Promptly reporting any incident using existing routes for reporting concerns.

Any incident of cyberbullying will be investigated under the appropriate policy and could result in disciplinary action.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Leeds City Council can accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling E-Safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the headteacher. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. Pupils and parents will be informed of the complaint procedure.

Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communications Policy

Introducing the e-safety policy to pupils:

- E-safety rules will be reminded and discussed with the pupils at the start of each year and every time the Internet is used.
- Pupils will be informed that network and Internet use will be monitored.

<u>Staff and the E-Safety policy</u>

All staff will be given access to the school e-Safety Policy and its importance explained.
Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. *(Please refer to the Acceptable Use Policy.)*

<u>Enlisting parents' support</u>

Parents' attention will be drawn to the school e-Safety in the school prospectus and on the school website.

E-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. At Holy Spirit Catholic Primary School we have ‘Think and Click’ E-safety rules for each of the three key stages (Foundation Stage, Key Stage One and Key Stage Two). This is to ensure all children of all ages are able to use the Internet safely and appropriately. Please find these rules attached for you to read. It is school policy for parents/carers to sign to show that the E-Safety Rules have been understood and agreed. We would really appreciate it if you could read and sign the consent slip below and return it to the school office as soon as possible.

Many thanks,

Mrs C Roberts Head teacher	Mr M O’Brien Head of school

Parent’s Consent for Internet Access
I have read and understood the school E-safety rules and give permission for my son/daughter 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.

Name of child: **Class:**

Signed: ***Date:***

Please print name:

Parent’s Consent for Web Publication of Work
I agree that my son/daughter’s work may be electronically published on the school website.

Name of Child: **Class:**

Signed: ***Date:***

Please print name: