Online Safety Policy

2025

Great Harwood St. John's CE Primary

"Where everyone shines with God's love"

based on "Let your light shine" Mathew 5:16

Online Safety Policy

We at St John's CE Primary School are committed to meeting the needs of our pupils and ensuring that they make progress. In line with our mission statement, we aim to:

Build a better place, where:

Everyone is welcome;

No one is ever lonely;

We respect and trust each other;

There is always someone to ask for help;

People help us to be the best we can.

Great Harwood St John's CE Primary School statement of intent

'Where everyone shines with God's love.'

As a Church of England school, our curriculum has Christian values at its heart. It is our intent at Great Harwood St John's that ALL learners leave our school with a lifelong love of learning and they know that they are loved and treasured as individuals. To enable them to do this our curriculum has been carefully designed around our children, celebrating differences and developing the uniqueness of each child. We recognise children's starting points and quickly set about developing their phonics, early reading and maths skills through first hand experiences. Throughout their journey with us at St John's, we shower the children with enrichment opportunities to broaden their horizons and enhance their curiosity about their local community and the world around them. Staff work collaboratively, utilising each other's expertise to ensure a clear, coherent, well-balanced curriculum made bespoke to us. Ultimately, the day-to-day decisions of the school are to ensure that the whole child's needs are met whether this is academic or social and emotional.

What is Online Safety?

Whilst the internet and associated technologies are an excellent tool and resource to enrich learning there are still dangers related to their use, especially in relation to young students. Some examples of these are:

- Bullying via chat or email
- Obsessive internet use
- Exposure to inappropriate materials
- Inappropriate or illegal behaviour
- Physical danger of sexual abuse

As a school it is our duty of care alongside that of parents and other members of the community to protect our children from these dangers and this can be achieved by many different mechanisms working together. The purpose of this online safety policy is to outline what measures Great Harwood St John's CE Primary School takes to ensure that children can work in an online environment and that any online safety issue is detected and dealt with in a timely and appropriate fashion.

General policy statement

Great Harwood St John's CE Primary School will endeavour to ensure the online safety of all personnel (including children). It will use education, technology, accountability, responsibility and legislation as the key ways to achieve this.

Whole School responsibilities for online safety

Within the school all members of staff and children are responsible for online safety, responsibilities for each group include:

Children

- Participating in and gaining an understanding of online safety issues and the safe responses from online safety training sessions.
- Compliance with a highly visible student's Acceptable Use Policy (AUP) which children must agree to each time they use school computing equipment either in the school or remotely which connects to the internet.
- Reporting any online safety issue to the teacher, team leader or parent.
- Take responsibility for their own actions using the internet and communications technologies.

All Staff

- Have a clear understanding of online safety issues and the required actions from online safety training sessions.
- Reporting any online safety issues to the computing subject leader/DSL as soon as the issue is detected.
- Compliance with a highly visible staff Acceptable Use Policy (AUP) which staff must agree to each time they use school computing equipment either in the school or remotely which connects to the internet.

Teaching Staff

- Educating children about online safety through specific online safety training sessions and reinforcing this training in the day to day use of ICT in the classroom

Network Manager (LancsICT support Nigel Smith)

- Deals with online safety breaches from reporting through to resolution in conjunction with the computing support team.
- Works with the computing subject leader and head teacher to create, review and advise on online safety and acceptable use policies.
- Works with outside agencies including the police where appropriate.
- Maintains a log of all online safety issues (passed on to head teacher).

How the school ensures online safety in the classroom

Educating children in online safety

- A clear objective of the school is to educate children in safe use of computing and the internet. We feel this is one of the best ways to minimise the potential for any online safety issues to occur.
- Children will receive specific online safety lessons aimed at ensuring that:
- Children know the online safety risks that exists and how to identify when they are at risk.
- Children know how to mitigate against online safety risks by using online safe practices whilst online.
- Children know when, how and to whom to report instances when their online safety may have been compromised.
- Children know that they are in an environment that encourages them to report online safety issues without risk of reprimand, humiliation or embarrassment.

In addition to this specific training all members of staff will have a duty to reinforce online safety practices wherever possible and will offer students advice and support in the classroom where minor online safety incidents have occurred.

Online safety education information will have high visibility in all areas of the school

How technology is used

The school will employ many different technologies to help to ensure online safety for all the school members;

- The school will use internet filtering to block inappropriate content and in addition block websites which are irrelevant to the student's programme of study and are considered time wasting.
- The school will use a system which tracks all student activity on the school's computers. This system will automatically flag potential online safety issues which will be monitored and then can be investigated by the support for learning team.
- The school will restrict which activities the children can perform using computing and the internet through systems security policy and access control.
- Teaching staff will use control mechanisms to attempt to limit the applications and web sites which the children can visit whilst using computing within a lesson.

How the School will respond to issues of misuse

The following are provided for the purpose of example only. Whenever a child or staff member infringes the Online Safety Policy, the final decision on the level of sanction will be at the discretion of the Head Teacher.

Children

- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites
- Accidentally accessing offensive material and not notifying a member of staff of it
- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email that is regarded as harassment or of a bullying nature
- Deliberately trying to access offensive or pornographic material
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

Staff

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Any deliberate attempt to breach data protection or computer security rules;
- Bringing the School into disrepute.

Possible Sanctions (for both staff and children)

Referred to Head Teacher /exclusion / removal of equipment / referral to police / LA online safety officer

Working with parents and the community

Clearly many school children will also have access to computing and the internet at home, often without some of the safeguards that are present within the school environment. Therefore, parents must often be extra vigilant about their child's online safety at home. One of the goals of the school is to support parent's role in providing an online safe environment for their children to work in outside the school. The school will do this in several ways;

- Publish online safety information and direct parents to external online safety advisories via the school website
- Use external agencies to support children in staying safe in the online safety environment.

This policy will be reviewed by the Computing subject leader on an annual basis.

Policy written and agreed by Staff and Governors – February 2025