# TRANMERE PARK PRIMARY SCHOOL

**RIDGE CLOSE
TRANMERE PARK
GUISELEY
LEEDS
WEST YORKSHIRE
LS20 8JJ**

**TELEPHONE: 01943 875050
FAX: 01943 871041
Email: secretary@tranmerepark.leeds.sch.uk**



# Online Safety Policy

# Adoption Date: Feb-18
# Review Date: Feb-21

*Tranmere Park Primary School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.*

## Introduction

Online safety encompasses all internet technologies and electronic communications such as mobile phones and tablets. The increased use of these technologies highlights the need for children to be educated about their risks and benefits and provides safeguards and awareness for children to be able to control their online experience.

Online safety is a safeguarding issue not an ICT or Computing issue and all members of the school community have a duty to be aware of online safety at all times, to know the required procedures and to act on them.

This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained by exploiting the benefits and opportunities by using ICT, whilst minimising any associated risks. It describes actions that should be put in place to redress any concerns about child welfare and safety as well as how to protect children, young people and staff from risks and infringements.

The Headteacher or, in her absence, the Deputy Headteacher or next member of the School Leadership Team, has the ultimate responsibility for safeguarding and promoting the welfare of pupils in their care.

This policy complements and supports other relevant School and Local Authority policies. The purpose of internet use in School is to help raise educational standards, promote pupil achievement, support the professional work of staff as well as enhance the School's management information and business administration systems.

## Ethos

It is the duty of the School to ensure that every child and young person in its care is safe. The same 'staying safe' outcomes and principles outlined in the Every Child Matters agenda apply equally to the 'virtual' or digital world. This expectation also applies to any voluntary, statutory and community organisations that make use of the School's ICT facilities and digital technologies.

Safeguarding and promoting the welfare of pupils is embedded into the culture of the School and its everyday practice and procedures.

All staff have a responsibility to support safe practices in the use of techology.

## Why we teach Online safety

### Why Internet use is important

The internet is an essential element for education, business and social interaction. The school offers provision to pupils to access the internet as part of their learning experience. It is also a resource for both staff and pupils.

### Benefits of Internet Use for Education

The internet is part of the statutory curriculum and as such, is a necessary tool for staff and children. It allows access to worldwide educational resources such as museums and galleries.

The internet also supports staff's continuing professional development through access to relevant frameworks, national policies and educational materials.

### Internet use will enhance learning

- The school internet access will be designed for pupils and will include appropriate filtering
- Pupils will be taught about acceptable internet use and will be given clear objectives for this
- Pupils will be taught effective use of the Internet for research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught how to evaluate Internet content
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

## Managing Internet Access

### Information system security

School ICT systems capacity and security are reviewed regularly. All internet access is filtered by the school's ISP and we will work together with them to ensure the efficacy of the filter as far as practicably possible. We recognise that no filter can ever be perfect, therefore, children will be taught the necessary skills to manage risks themselves on an age appropriate level.
Virus protection is updated continuously and a full scan is run daily.

### E-mail

- Pupils may only use their Office 365 e-mail account in school
- The Office 365 email system only allows communication within the school community.
- Pupils must immediately tell a member of staff if they receive an offensive email.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone they do not know personally
- The forwarding of chain mail is not permitted.

### Published content and the school website

The contact details on the school website should only include the school's e-mail address, address and telephone/fax number. The SENCO's email address is also published in line with best practice. Pupil and staff e-mail addresses will not be published.

The Headteacher will take overall responsibility for checking the accuracy and appropriateness of the content of the website.

### Publishing pupils' images and work

Written permission will be obtained from Parents/Carers on entry, before photographs of children are placed up on the school website. Pupil's full names will not be used on the school website, particularly in association with photographs.

### Social networking and personal publishing

- The School Network blocks/filters access from most social networking sites.
- Despite this, we will educate children on the safe use of these technologies as we are aware that our learners may choose to access these resources outside of school.
- Newsgroups are blocked unless a specific use is approved.
- Pupils will be advised never to give out any personal details which may identify them or their location.

- Pupils and parents will be advised that use of social networking sites outside of school is inappropriate for primary aged pupils, and further information will be provided to parents regarding this.

## Managing Filtering
The school will work with Schools Broadband (or any future ISP) to ensure that systems to protect pupils are reviewed and improved.
If staff or pupils discover an inappropriate website it must be reported to the designated safeguarding lead.
The network manager, alongside staff, will ensure that regular checks are made to ensure that the filtering methods selected are effective, appropriate and reasonable.

## Managing emerging technologies
- Emerging technologies will be examined for educational benefit and children will be supervised and monitored when using these.
- Mobile phones are not to be used during school hours. The sending of abusive or inappropriate text messages is strictly forbidden.
- Children will be educated about the risks inherent in the use of social messaging apps as we are aware that they will use these outside of school.
- Staff will be issued with a school phone if contact with pupils is required.

## Managing data security
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the General Data Protection Regulation 2016.

## Policy decisions
- All staff and governors must read and sign the 'Acceptable Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff/pupils who are denied internet access. The record will be kept up to date.
- In Key Stage 1, access to the internet will be under direct supervision, with access to approved online materials.
- Parents/Pupils will be asked to sign and return a consent form on their child's behalf.

## Assessing risks
The school will take all reasonable precautions to ensure that users only access 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 Schools Broadband can accept liability for the material accessed, or any consequences of Internet access. Methods to identify, assess and minimise risks will be reviewed regularly.

The school will audit ICT provision to ensure that its content is appropriate and its implementation effective.

## Handling Online safety complaints
- Complaints of Internet misuse and/or Online safety will be dealt with by the school's designated safeguarding lead.
- Any complaint over staff misuse should be referred to the Headteacher.

- Complaints of a child protection nature will be dealt with in accordance to school child protection procedures.
- Responses to internet misuse will include informing parents/carers of the incident.
- Further sanctions may include the removal of internet/computer access for a set period of time.

**Communications Policy**

Introducing the Online safety policy to Pupils
- Acceptable use posters will be positioned in all rooms where computers are used and discussed with pupils throughout the school year.
- Pupils will be informed that Internet use will be monitored.
- Regular online safety lessons and/or assemblies will be given.

Staff and the Online safety policy
- All staff will be given the Online safety policy and its importance explained.
- Staff will be aware that Internet use can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- All staff will receive child protection and Online safety training regularly

Enlisting parents' support
- Parents' attention will be drawn to the school's Online safety policy in newsletters and on the school website.
- A partnership approach will be encouraged, through use of parent ICT evenings and information on safe home Internet use.

Please refer to these additional policies to supplement this one: computing, acceptable use, equal opportunities, SEN, EAL and Gifted and Talented.