## Dringhouses Primary School

# E-Safety Policy

| | |
|---|---|
| **Signature of Chair of Governors** …… | |
| **Signature of Headteacher** …… | |
| **Date of Adoption** | **January 2022** |
| **Date of Review** | **January 2025** |
| **Reviewing Committee** | **Resources Committee** |
| **Statutory / Non Statutory** | |

# E-SAFETY POLICY

## Rationale

At Dringhouses Primary School, all staff, pupils, parents and governors seek to promote the safe and sensible use of computers, respecting the wishes and the privacy of all school users. We want our pupils to be aware of what to do if they come across offensive material or any inappropriate content, and to understand how to take care of themselves in an ever developing world of technology.

As a school, we strive to protect pupils from accessing inappropriate or offensive material whilst on the school site whilst ensuring that children are equipped with the knowledge they need to protect themselves from such material in other settings.

## Objectives

**Pupils and staff should be able to make use of a range of computer tools in school without fear of:**

- exposure to unpleasant, extremist or offensive material
- cyber-bullying from someone known or unknown
- contact from potential abusers
- physical harm caused by faulty or mismanaged computer equipment
- physical harm caused by poor posture at the keyboard
- invasion of privacy
- misuse of equipment

**We believe we have a responsibility to raise parents' awareness about the risk of:**

- exposure to unpleasant, extremist or offensive material online
- cyber-bullying from someone known or unknown
- young people disclosing personal details on social networking sites, or indeed anywhere online
- contact from potential abusers
- the unsupervised use of mobile devices
- games that can be accessed online by young people where they have the risk of exposure to unpleasant, extremist or offensive content.

## General Safe Use Procedures

1. All pupils are asked to sign an 'Acceptable Internet Use/E-Safety Agreement' as they start school, agreeing to abide by the school's policy and expectations. In the case of early years'/KS1 pupils, we ask parents to sign the document on their child's behalf. For this reason, as they enter KS2, pupils are re-issued with this agreement and asked to sign it again, once they are fully responsible for their own actions.

2. School devices (such as laptops, chromebooks and tablets) that have access to the internet should be used under careful teacher supervision/monitoring.

3. Teachers closely monitor children whilst they use the computers in lessons and clubs within school.

4. Pupils are required to sign into the internet, which is controlled by City of York Council and uses a safety filter to screen out sites that may have inappropriate content, including extremist material. Filtering is not 100% infallible, so pupil access to the Internet is always supervised. Class teachers have access their pupils' logins.

5. The school uses child-friendly sites (Purple mash, BBC Schools, Active Learn Primary, TTRockstars) and search engines (such as Kidrex) to assist in protecting users from accessing inappropriate material. Where possible, websites that are being accessed in the lessons will have been vetted by their teacher beforehand. However, children are also taught how to respond to inappropriate situations on the internet wherever or whenever they occur.

6. Staff and pupils do not upload data from outside the school onto school equipment without seeking approval from the class teacher, computing subject leader or one of the supporting technicians.

7. In the event that children should come across online material that they are unsure of, do not like, or feel is offensive, they are taught to:

    - Minimise or turn the screen off immediately
    - Put up their hand and tell a trusted adult.

8. Sanctions for behaviour that does not withhold this policy, will be in accordance with the school's Behaviour Policy.

9. In all such cases of abuse of the E-Safety Policy, or suspected cases, a child's parents will be informed immediately by the class teacher.

10. Workshops are offered to parents to inform them about the SMART approach to e-safety. The school will also hold annual 'E-safety weeks' which will coincide with the national event, 'E-safety Day' where the children will take part in E-safety assemblies, lessons and workshops.

11. Children are made aware of the potential hazards of using the Internet, including mobile devices. They are taught, in age specific lessons, to:

    - Ask a responsible adult before downloading any material
    - Seek help before clicking on any pop-up message that appears
    - Share their internet experiences and interests with their parents/guardians
    - Communicate any incident/image/message that makes them feel uncomfortable or endangered in any way with a trusted adult
    - Be aware of the points outlined above and take responsibility for ensuring their own e-safety
    - Understand the dangers of giving out any personal data on any internet site or application (including social networking sites, gaming sites, gaming consoles and messaging services)
    - Recognise incidents of cyber bullying and report them immediately
    - Understand who they can report incidents of cyber bullying to

- o Realise that some internet content may be unsuitable, inaccurate or only represent a certain point of view.

12. Children should only log into their own user areas on the computers.

13. No offensive or extremist words or terms will be input into folders or search engines by any person.

14. No offensive or extremist material will be accessed or downloaded by any person.

15. Confidential information should only be accessed on encrypted devices (such as school laptops).

16. Content from the school server is backed up on a daily basis. Computer support is provided by VITAL (York) Ltd.

17. Children are taught e-safety as a strand of computing. The principles of this are recapped before school holidays, when children may be accessing the internet unsupervised.

**Use of Cameras**

Children and staff may use cameras, video cameras and ipads to record children for educational purposes. Each class is provided with its own ipad, which should be used exclusively for school purposes. Cameras, recording equipment and ipads are not to be taken off school property by any child.

**Data Storage and Transfer**

It is recognised that staff may need to store information and transfer data between home and school, including occasional images. The storage of sensitive data is strongly discouraged and it is suggested that such information is sent via secure e-mail and then deleted. This includes assessment data, images and reports.

Where data of a personal nature is taken home on an encrypted school laptop, it must be recognised that this data comes under the Data Protection Act and is subject to the school's Data Protection Policy. Care must therefore be taken to ensure its integrity and security. No data of a personal nature should be transferred onto home computers or stored on any portable device.

**Personal data** is defined as data which relates to a living individual who can be identified:
(a) from the data, or
(b) from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller

**Mobile Phones**

Most mobile phones have access to the internet and picture and video messaging. They present opportunities for unrestricted access to the internet and sharing of images and present risks of cyberbullying and inappropriate content. The sending of abusive, offensive, extremist or inappropriate material is forbidden.

Staff, including student teachers, volunteers and visitors, are not permitted to access or use their mobile phones within the classroom during teaching hours. They may use them during break and lunch periods. Staff should always use a school phone to contact parents. Staff may take mobile phones on educational visits, but they must only be used to take photographs for posting on Twitter or for educational use back in school, or in the event of an emergency. Any images or videos of pupils or staff taken on mobile phones will be deleted immediately after they have been posted to Twitter or saved elsewhere on the school's encrypted drive. Staff who do not adhere to this policy will face disciplinary actions.

Pupils in KS2 may bring mobile phones into school, however these must be handed in to the classteacher before registration and collected at the end of the day. The school accepts no responsibility for the safekeeping of children's mobile phones whilst on the school premises.

Parent helpers on educational visits are not permitted to use their mobile phones to take pictures of the children.

**The School Website**

When considering material for publication on the internet, Dringhouses Primary School ensures that parents are informed of the school's policy on taking and publishing images, and that pupils' full names are not published on the website unless parental consent has been given. More information on this is included in the 'Using Images' policy.

**Social Networking**

**Pupils and parents** are advised that only moderated social networking sites should be used for primary age children and that the minimum age for accessing most well-known social networking sites is 13. Pupils are advised never to give out personal details which may identify them or their location and not to place personal photos on any social networking sites. Pupils are also advised to look at their privacy settings with an adult to ensure that they are suitable. The school encourages parents to know their child's passwords to allow them to check the suitability of content on their social networking accounts.

**Staff and volunteers** are reminded that it is inappropriate to discuss issues relating to children or other staff via social networks and are encouraged to review their privacy settings to ensure that their profiles and photographs are not viewable by the general public. It is not acceptable for staff to accept a friend request from a child at the school or a former pupil, or from parents who are not already friends outside of school. The Staff Code of Conduct gives further social networking guidelines.

**Responding to a violation of the e-safety policy.**

Should anyone find themselves a victim of, or a witness to, an incident that violates these e-safety rights, we encourage them to make the headteacher or computing subject leader aware.

Any serious incident involving the use of computers on or off site, which is reported to school staff, will be handled with due regard to the school's Safeguarding and Child Protection Policy or, as appropriate, the Behaviour Policy and Data Protection Policy.

Any breach of the Staff Code of Conduct will be handled through the school's Disciplinary Procedures.

Any allegation against a member of staff will be handled through the Complaints Procedure or Whistleblowing policy.

Despite the type of precautions set out in this policy, it is clear that no school can give 100% guarantee to parents that no inappropriate material will ever occur in school. It is important, however, that staff, pupils, parents and governors take every possible step to try to ensure that it never happens. Should these steps fail to prevent an abuse of Safe Use procedures, it is understood by all that the strongest steps will be taken against any offender.

# Pupil Acceptable Internet Use /E-Safety Agreement

**Computing, including using the internet, has become an important part of learning in our school. We expect all children to be safe and responsible when using computers. Please read and discuss these E-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns, or would like some explanation, please contact your child's class teacher.**

- I will only use computers in school for educational purposes or tasks set by a trusted adult.
- I will not tell other people my passwords (including my log-ins for TTRockstars, Abacus and Purple Mash).
- I will only log onto my own user area on the computer and open/edit my own files.
- I will check with my class teacher before deleting any of my own files.
- I will make sure that all computer and internet contact with other children and adults is responsible, polite and sensible.
- I will not download anything onto the school system without permission.
- I will not deliberately look for, save or send anything that is inappropriate, or could be unpleasant or offensive. If I accidentally find anything like this I will turn off my screen and tell my teacher immediately.
- I will ask for help from a trusted adult before clicking on any pop-up message that appears.
- I will not give out my own details such as my name, phone number or home address anywhere online.
- I know that my use of computers can be checked and that my parents/carers will be contacted if a member of school staff is concerned about my E-Safety.
- I will be responsible for my behaviour when using computers because I know that these rules are to keep me safe.

……

**DRINGHOUSES PRIMARY SCHOOL**
**ACCEPTABLE INTERNET USE / E-SAFETY AGREEMENT**

Child's Name …… Class ……
We have discussed this agreement and ……(child's name) agrees to follow the E-Safety rules and to support the safe use of computers at Dringhouses Primary School.

Signature of Parent/Carer …… Date ……

Signature of Child …… Date ……
***(parent/carer to sign on behalf of children in Early Years/Y1/Y2)***