endeavour multi academy trust

Tamworth Nursery

TWO RIVERS PRIMARY SCHOOL

Cherry Trees School

TWO RIVERS HIGH SCHOOL

W.H.S.

E-Safety Policy

Two Rivers High School

Review date: Spring Term 2021

Next Review: Spring Term 2022

Introduction

At Two Rivers High School we take internet safety very seriously and see it as our duty to keep our pupils safe whilst using technology not only in school but also at home.

The policy covers three main areas; children's safety, staff's responsibilities and support for parents.

E-Safety Committee

An E-Safety Committee has been set up which includes, the ICT Teachers, a nominated Governor, IT Support Team and a member of the school Senior Leadership Team.

The group's responsibility is to annually review the E-Safety Policy and curriculum. The group meets twice a year. Minutes are taken which are available in the E-Safety Folder in Two Rivers ICT Department shared space on the learning platform. A hard copy is located in the E-Safety Folder.

Network Safety

The school's network is presently managed by the in-house support team who are responsible for the safety of the network and the pupils / staff who access it.

Termly meetings takes place with representatives of the IT Support Team and representative of the Senior Leadership Team. During this meeting any issues with the network and E-Safety issues are dealt with.

Future Digital Policy Central, which is a highly effective monitoring system which identifies cyberbullying and other safeguarding concerns, is used in school as part of the Local Authority's support for E-Safety. This is checked weekly by the Senior Leadership Team. Issues that are highlighted in these checks are then dealt with by the Senior Leadership Team.

Safety and Responsibilities for Staff

All staff are required to read and electronically sign an Acceptable User Policy (AUP) which clearly states the responsibilities of staff using technology in the work place. This will be signed when they commence their employment at Two Rivers and will be re-enforced monthly.

The AUP list the responsibilities of all staff and covers the use of digital technologies in school: i.e. e-mail, internet, intranet and network resources, learning platform, software, equipment and systems and complements the General Teaching Council's Code of Practice for Registered Teachers.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Headteacher and the Local Governing Board.
- I will not reveal my password(s) to anyone. I will not log on for another person.
- I will not allow unauthorised individuals to access e-mail / internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I understand that there is a difference between my professional and private roles. I will not engage in any online activity that may compromise my professional responsibilities, this refers to social network sites such as Facebook. (Refer to Staff Code of Conduct and Social Media Policy)
- I will only use the approved, secure e-mail system(s) for any school business.
- I will only use the approved school e-mail, school learning platform or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- At any time I will not use school equipment to browse, download or send material that could be considered offensive or inappropriate to colleagues or pupils.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Headteacher.
- I will not download any software or resources from the internet that can compromise the network or are not adequately licensed.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personally owned digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home. (see Mobile Phones, Camera and Image Policy and Procedures)
- I will use the school's learning platform in accordance with school / and Northern Grid for Learning advice.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer, laptop or i-Pad loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school if a reasonable amount

of personal use outside of school hours becomes "significant personal use" as defined by HM Revenue & Customs.

- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection guidelines require that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's E-Safety Curriculum into my teaching.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage / and network usage is monitored and that monitoring data could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

E-Safety training will be provided to all members of staff once a year and it is each person's responsibility to attend this session. These sessions will be arranged by the ICT Coordinator.

It is very important that staff make sure that pupils they are responsible for are using the internet safely.

Primary and High School share Facebook and Twitter accounts. Each school post information and pictures in line with Media and Information Sharing Policy. Access to both profiles are available only to the Senior Leadership members and ICT Technicians to quality assure the items posted online. A permission is gained from parents/carers to enable their child to be featured on Facebook and Twitter.

Safety and Responsibility for Pupils

Although some of our pupils are unable to access the internet we have a good percentage of pupils who are able to use the internet independently and therefore are at risk from either deliberately accessing inappropriate material or, due to their level of literacy, accidently accessing harmful sites.

No child is able to access the internet in school without their parents giving permission to do so. This consent form is filled in when the child starts school and is kept on record until they leave; it will only need amending if a parent/carer would like to change it.

All pupils who are able will have to sign an AUP and this will be completed every year during the students E- Safety session. This document will clearly state their responsibilities when using technology in school.

All pupils will receive E-Safety training at the beginning of each term as part of their ICT lesson.

All pupils will be taught how to use all technologies in a responsible and safe way. This will be part of the ICT Curriculum. Internet safety aspects are also taught in PSHE lessons as part of the accredited AQA course.

No child may appear on the website without their parent/carer's consent, the consent form is completed when the child starts school and is kept on record until they leave; it will only need amending if the parent/carer would like to change it.

Support for Parents/Carers

As a school we believe it is our duty to support parents and carers in keeping their child safe while using technology within the home environment. Computers and other devices in the home are more open and don't have the security features which we have in school, which does make the child more vulnerable in this environment.

The parents will be invited to E-Safety sessions which will be held in school at the beginning of the school year. Two sessions will be offered one during the school day and the other after school.

The school website will have information regarding E-Safety for parents/carers and young people.

E-Safety topic is one of the focuses for Parents Seminars at High School.

Remote Learning

Devices on loan for remote learning have been equipped with Smooth Wall Monitor software to ensure inappropriate use or access to materials not suitable to the age of the child are logged and recorded. Monitoring of this is conducted by the Headteacher. Parents are required to sign an AUP before the loan is secured.