Wellspring Academy Trust
E-Safety Policy
May 2015

Date Approved by Board: 20 May 2015

Who this policy applies to:

-

Date of Review: May 2018

Responsible Department: Wellspring Head Office

1. Introduction

1.1. At Wellspring, we recognise that learning is a lifelong process and that e-learning is an integral part of it. Ensuring that we provide pupils with the skills to make the most of information and communication technologies is an essential part of our curriculum. We are committed to the continuing development of our ICT infrastructure and embracing new technologies so as to maximise the opportunities for all pupils, staff, parents and the wider community to engage in productive, cooperative and efficient communication and information sharing.

1.2. Academy E-Safety policies should apply to all stakeholders of the Academy community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of Academy ICT systems, both in and out of Academy, and acknowledge that the Education and Inspections Act 2006 empowers Principals, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the Academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

Roles and Responsibilities

2. Governors

2.1. The Governors of the Academy are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

3. Principal and Senior Leaders

3.1. The Principal is responsible for ensuring the safety (including e-safety) of members of the Academy community, though day to day management of esafety may be delegated to the Designated Lead for Safeguarding and ESafety.

3.2. The Principal must ensure that the Designated Lead for Safeguarding and E-Safety and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues as deemed appropriate.

3.3. The Principal and will ensure that there is a system in place to allow for monitoring and support of the Designated Lead for Safeguarding and E-Safety.

3.4. The Principal must be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

4. Education and Training - Staff

4.1. It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in the Academy E-Safety policy.

5. Training Governors

5.1. E-Safety awareness sessions will be offered to members of the governing body.

6. Technical – infrastructure, equipment, filtering and monitoring

6.1. The Academy will be responsible for ensuring that the Academy infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved are implemented.

7. Use of digital and video images

7.1. The Academy is responsible for the safe use of photographic and video images of all pupils.

8. Data Protection

8.1. Personal data should be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

8.1.1. Fairly and lawfully processed
8.1.2. Processed for limited purposes
8.1.3. Adequate, relevant and not excessive
8.1.4. Accurate • Kept no longer than is necessary
8.1.5. Processed in accordance with the data subject's rights
8.1.6. Secure
8.1.7. Only transferred to others with adequate protection.

9. Communications

9.1. When using communication technologies the Academy should give due consideration to safety and security.

Responding to incidents of misuse

10. Staff

10.1. The Academy should make provision for dealing with the purpose of equipment and internet by pupils and staff.