1. Introduction

1.1 At Overley Hall 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.

1.2 This document has been written in conjunction with Telford and Wrekin E-safety guidance.

1.3 The policy covers three main areas: Children's safety, staff's responsibilities and support for parents.

2 E-Safety Committee

2.1 An E-Safety Committee has been set up which includes, the Head of School, Head of Care, Start technician, ICT teacher, Deputy Head of School & Assistant Head of School.

2.2 The group's responsibility is to annually review the E-Safety policy and curriculum. The group will meet termly and minutes will be taken which will be available in the E-Safety folder, and kept in the Head of School's office. Minutes will be emailed to every member of staff.

3 Network Safety

3.1 The school's Network is presently managed by Start Technology who are responsible for the safety of the Network and the pupils/staff that access it.

3.2 A fortnightly visit takes place with representatives of the Start technical team, and any issues with the Network and E-Safety are dealt with. Staff make requests on forms and are presented via the Head of School to Start to address. Software can only be installed on computers by administrators (Start Technology). If a member of staff requires software to be installed onto computers a change request form is required to be completed and signed by Bev Doran.

3.3 K9 web protection is currently installed to pupil laptops and family unit PC's. This enables us to block adult theme sites containing adult material.

3.4 ESET Anti-virus is installed on all computers, laptops and server to defend against viruses and potential threats.

3.5 Policy Patrol mail security is installed on the server which filters out spam emails and potential dangerous attachments for all users. Selected staff have requested exclusion from Policy Patrol.

3.6 Staff and students have individual computer login accounts; Staff have email accounts configured on their login. Staff and students can access server documents if permission is granted. A 'change request' form needs to be agreed and signed by Head of School for this to happen.

4 Safety and Responsibilities for Staff

4.1 All staff are required to read and sign an Acceptable User Policy (AUP) which clearly states the responsibilities of the staff using technology in the work place. This will be signed when staff commence their employment at Overley Hall School and will be re-enforced every two years during the staff's biannual E-Safety session.

4.2 The AUP lists the responsibilities of all staff and covers the use of digital technologies in school: email, internet, intranet, resources, software, equipment and systems that complement the General Teaching Council's Code of Practice for Registered Teachers.

5 AUP

5.1 I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head of School.
5.2 I will not reveal my password(s) to anyone. I will not log on for another
5.3 I will not allow unauthorised individuals to access:
E-mail/Internet/Intranet/Network
5.4 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.
5.5 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.
5.6 I will only use the approved, secure E-mail, and other approved communication systems with pupils or parents/carers, and only communicates with them on appropriate school business.
5.7 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.
5.8 I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Head of School or Head of Care.
5.9 I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
5.10 I will not connect a computer, laptop or other device (including USB flash drives), 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.

5.11 I will not use personally owned camera phones for taking and transferring images of pupils or staff without permission for HoS and will not store images at home.

5.12 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.

5.13 I agree and accept that any computer, laptop or IPad loaned to me by the school, is provided solely to support my professional responsibility's 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.

5.14 I will ensure any confidential data that I wish to transport form one location to another is protected by encryption and that I follow school data security protocols when using such data at any location.

5.15 I understand that data protection policy requires 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.

5.16 I will embed the school's E-safety curriculum into my teaching and practice.

5.17 I understand that all Internet usage/and network usage is monitored and that monitoring data could be made available to my Head on request

5.18 I understand that failure to comply with this agreement could lead to disciplinary action.

5.19 E-Safety training will be provided to all members of staff once every two years and it is each person's responsibility to attend this sessions. These sessions will be arranged by the Head of School.

5.20 It is very important that staff make sure that pupils they are responsible for are using the Internet safely. High risk students will be highlighted by the E-Safety team and staff will be made aware of these students' names.

6 Safety and Responsibility for Pupils

6.1 Although many of our pupils are unable to access the Internet without a great deal of support a small percentage of pupils are able to access 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.

6.2 All pupils for whom it will be meaningful will receive E-Safety training at the beginning of each term as part of their PCD lesson and will be delivered in a way which be meaningful and relevant.

6.3 Pupils and young people for whom it will be meaningful will be taught how to use technologies in a responsible and safe way. This will be part of the ICT curriculum. This training will be presented in Widgit format to ensure maximum understanding. A set of SMART (Safe, Meeting, Accepting, reliable and Tell) rules will be displayed in classrooms near to computers where students who will be able to access the Internet are located. ICT will be delivered cross curricularly at Overley Hall School.

6.4 Pupils and young people with Autism are vulnerable as they cannot always see the bigger picture. Deficit of 'theory of mind' makes it hard for them to determine another person's thinking and/or intentions therefore it is vital that a high level of support is given to protect those who can access the internet. Dynamic risk assessment is crucial.

6.5 No child may appear on the Web Site without their parent/carers consent which is completed when the pupil starts at school and is kept on record until they leave. It will only need amending if the parent, carer would like to change it.

7 Support for Parents

7.1 As a school we believe it is our duty to support parent 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 more vulnerable in this environment.

7.2 The parents will be invited to E-Safety sessions which will be held at school at the beginning of the year. These will be offered as twilight sessions.

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

7.4 Monthly 'drop in' sessions are on offer for parents to discuss E-Safety with the Head of School and the Head of Care.

I (name)_____ agree to abide by this E-Safety Policy and Acceptable Usage Policy.

Signature_____ Date _____