Introduction

At Overley Hall, we take online safety very seriously and see it as our duty to keep the children and young people safe whilst using technology.

This document has been written in conjunction with Telford and Wrekin Online-Safety guidance. This policy must be taken in consideration with GDPR (general data protection regulations), Data protection Policy, Personal Mobile Phone and Bring Your Own Device (BYOD) Policy and the Blog and Social Networking Policy and Procedure.

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

Rationale

As pointed out in 'Keeping Children Safe in Education' (DFE Sept 2019)… "The use of technology has become a significant component of many safeguarding issues", "…technology often provides the platform that facilitates harm" and that organisations like Overley Hall must 'protect and educate' children and young people in 'safe use of technology' whilst establishing "…mechanisms to identify, intervene in, and escalate any incident where appropriate". Furthermore, they suggest the vast risks to be considered can be classified into 3 areas:

1. **Content**: exposure to illegal, inappropriate or harmful material (pornography, extremism, etc.)
2. **Contact:** experiencing harmful online interaction with other users (adverts or even adults posing as children)
3. **Conduct**: increased risk of harm due to their online behaviour (online bullying, sending or receiving explicit images)

At Overley Hall we recognise that the television, iPad, internet and use of computer can provide young people with invaluable access to communication and leisure experiences. However, when using the internet there are risks in regards to child exploitation, viewing inappropriate materials and possible hate crimes. This policy therefore also aims to support staff to have wider knowledge when young people are using electronic devices and the internet.
This policy is also in support of Regulation 7 (The children's wishes and feelings standard), Regulation 10 (The health and well-being standard) and Regulation 12 (The Protection of Children Standard).

Safety and Responsibility for Pupils

Although many of our children or young people are unable to access the Internet without a great deal of support a small percentage of pupils are able to access the

internet independently. It is therefore important to recognise and be aware of the risk associated with children or young people either deliberately accessing inappropriate material or, due to their level of literacy, accidently accessing harmful sites.

All young people or children, for whom it will be meaningful, will receive Online-Safety training and further training if or when required on a needs based process in line with learning level needs or requirements.

Children and young people, for whom it will be meaningful, will be taught how to use technologies in a responsible and safe way. This will also be included within the schools' computing curriculum for those learners that are on roll. Maximum understanding will then be ensured during training whilst utilising appropriate resources or strategies such as 'Writing with Symbols' (WWS). Visual support will be used where ever appropriate to enable children and young people to safely access the internet.

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.

Although proactive strategies are in place, staff will also be required to monitor internet usage to enable dynamic risk assessments whilst ensuring and maintaining the safety of children and young people. Staff are required to carry out dynamic risk assessments to ensure the protection of individuals from accidental/intentional access to websites or material with the potential risk to cause emotional harm.

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

Online-Safety Committee

An Online-Safety Committee has been set up which includes, the Principal, Start technician, Computing tutor and Head of Education.

The group's responsibility is to annually review the Online-Safety policy and curriculum.

Network Safety

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

A fortnightly visit takes place with representatives of the Start technical team and any issues with the Network or Online-Safety can be dealt with. Staff can make requests or raise issues using forms, email or/and by speaking directly to someone from the senior leadership team, where Start can be informed and a 'Ticket' raised so the issue can be addressed. Software can only be installed on computers by administrators (Start Technology). If a member of staff requires software to be installed onto computers a request form or email will be required to seek approval from the leadership team.

K9 web protection is currently installed on pupil laptops and family unit PC's. This enables us to monitor usage. 'Web Titan' is then used as a proxy server to block anything deemed inappropriate such as adult themed sites containing adult material.

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

Policy Patrol mail security is installed on the server which filters out spam emails and potential dangerous attachments for all users.

Staff, children and young people have individual computer login accounts; Staff have email accounts configured on their login. Staff, children and young people can access server documents if permission is granted. In order for this to happen, staff, children or young people will require confirmation from the senior leadership team.

For Online-Safety purposes, staff, children, young people and anyone accessing Overley Hall's services should never connect or try to connect a PC or laptop which has not been verified by 'Start Technology' as this would jeopardise the safety of the Network.

Any separate devices that are able to connect to the network must be brought to the attention of the senior leadership team where permission must be granted and safety precautions then followed. This would include enabling Wi-Fi access, accounts specifically linked to Overley Hall or considering alternative strategies that maintain the safety of the children and young people. An example of this would be about configuring a 'PlayStation' so that it can only access material appropriate for the individual child or young person using it.

Anyone accessing Overley Hall's internet services must refrain from using personal accounts such as 'Netflix' or 'Amazon Prime' where less restrictions can put people at greater risk. Where such applications are required, approval must be pursued, strategies considered and accounts solely purchased through Lynn Thompson or a senior leader such as the Principal or registered manager.

If required, anyone visiting Overley Hall such as Social workers or Doctors can be granted temporary access to the internet, through our 'guest' network, by Lynn

Thompson or by her responsible designated person. A protocol will be signed to ensure Online-Safety.

Policy for Young People

Overley Hall will always provide electronic communication aids.
Young people will be expected to use the internet safely and staff will offer guidance in regards to this, however if we suspect young people are possibly communicating with strangers they will be given appropriate support in keeping with risk assessments and support plans, therefore greater vigilance will be required.

If young people post blogs, comments, videos etc., online, the senior leaders will monitor such actions for appropriateness and possible abusive interactions which may be received.

The senior leadership team will not automatically stop young people from posting online, however this will be thoroughly assessed and reviewed frequently.

Safety and Responsibilities for Staff

All staff are required to read and sign an Acceptable User Policy (AUP, see Appendix A) 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 and will be re-enforced every two years during the staff's biannual Online-Safety session.

The AUP lists (see Appendix A) the responsibilities of all staff and covers the use of digital technologies in Overley Hall such as email, internet, intranet, internet TV, resources, software and equipment. This includes the use of 'Behaviour-Watch', our online reporting system for incidents, accidents, body maps and significant or positive events.

Support for Parents

As a company we believe it is our duty to support parent and carers in keeping their child safe while using technology within the home environment. We therefore aim to provide parents with up-to-date information via our website or in person / training to help provide them with sufficient information to keep everyone informed and safe.

This policy will be made available for parents, carers and relevant professionals which will provide supportive information to keep their children and young people safe.

The parents will be invited to Online-Safety sessions which will be held at the school.

Overley Hall website will have information regarding Online-Safety for parents/carers and young people.

Monthly 'drop in' sessions are on offer for parents to discuss Online-Safety matters with the Principal or Head of Education. We also offer an open door policy.

Online-Safety training will be provided to all members of staff on a regular basis as part of child protection and safeguarding training with specific training provided once every two years and as deemed necessary.

It is very important that staff make sure that the children and young people with whom they are responsible for, are using the internet safely. Positive Support Plans will highlight those that present a higher risk and specific risk assessments put in place.

Appendix A

AUP

- I will only use Overley Halls' digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the senior leadership team.
- I will escalate any concerns regarding children or young people being exploited or abused online immediately to a DSL such as the Principal or Registered Manager.
- I will not reveal my password(s) to anyone or not log on for another to use.
- I will not allow unauthorised individuals to access: E-mail / Internet / Intranet / Network / BehaviourWatch.
- I will ensure all documents, data, etc., are saved, accessed and deleted in accordance with Overley Hall's network, data security and confidentiality protocols.
- At any time I will not use Overley Hall's equipment to browse, download or send material that could be considered offensive or inappropriate to colleagues or pupils.
- I will report any accidental access, or receipt of inappropriate materials, or filtering breach to one of the senior leadership team members.
- 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 drives), to the network/internet that does not have up-to-date anti-virus software and will keep any 'loaned' equipment up-to-date, using Overley Hall's recommended anti-virus, firewall or other ICT 'defence' systems.
- I will not use personally owned camera phones for taking and transferring images of pupils or staff and recognise that only in special circumstances, such as emergency situations would a phone be used for such purposes, providing senior leadership permission has been received.
- I will ensure that any private social networking sites or blogs are not used to comment or discuss information relating to the Overley Hall or work colleagues (this includes being aware of personal information posted by others which may bring their conduct into question).
- I will not use personal e-mail addresses, instant messaging identities and social networking accounts for company communication.

- I will not use personal home/mobile telephone numbers for contacting parents or cares.
- I will only use approved and secure e-mail or other approved communication systems, with pupils or parents/carers for appropriate 'work' business purposes.
- I will not access social media at work or on company computers or phones.
- I understand that there is a difference between my professional and personal life and will therefore not engage in any online activity that may compromise my professional responsibilities. This refers to social networking sites such as Facebook, Instagram or Twitter.
- I agree and accept that any computer, laptop or iPad loaned to me by Overley Hall, is provided solely to support my professional responsibility's and that I will notify the senior leadership team if a reasonable amount of personal use outside working hours become 'significant personal use' as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport form one location to another is protected by encryption and that I will follow Overley Hall's data security protocols when using such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within Overley Hall'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 Overley Hall's Online-Safety policy into my working day practice.
- I understand that all Internet or network usage at Overley Hall is monitored and data could be made available to the senior leadership team on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

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

Signature_____ Date _____