Wickersley Partnership Trust eSafeguarding Policy

"Inspiring today's children for tomorrow's world"

This policy has been written in accordance with YHGfl guidance, licenced under a Creative Commons Attribution-Non Commercial-Share Alike 3.0 Unported License

Vision, Scope and Ownership

At Aston Lodge Primary School, our mission statement focuses on inspiring today's children for tomorrow's world; therefore, it is crucial to prepare them to safely use a range of technologies. The objective of this policy is to safeguard and protect the children and staff belonging to the Wickersley Partnership Trust, and equip them with the necessary skills and knowledge to protect themselves online. Furthermore, the policy aims to assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice, and to set clear expectations of behaviour and codes of practice relevant to responsible use of the internet for educational, personal or recreational use.

This policy applies to the whole school community including both schools' Senior Leadership Team, local board of governors, all staff employed directly or indirectly by the school and all pupils.

The school eSafeguarding policy has been agreed by the senior leadership team and approved by governors. The eSafeguarding policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school. The School has also appointed link governors for 'Behaviour and Safety' to take the lead responsibility for eSafeguarding.

Title	Aston Lodge Primary
Version	2.0
Date	January 2020
Approved by head teacher	Sarah Cronin
Approved by Safeguarding body	Sarah Cronin, Amanda Howarth-Smith
Approved and shared with staff	January 2020
Next Review Date	January 2021

Policy Communication

The senior leadership team at Aston Lodge will be responsible for ensuring that all members of school staff and pupils are aware of the existence and contents of the school eSafeguarding policy and the use of any new technology within school. The eSafeguarding policy will be provided to and discussed with all members of staff formally, and will also be made available for all members of staff on the school network. All amendments will be published and awareness sessions will be held for all members of the school community. An eSafety module will be included in the curriculum covering and detailing amendments to the eSafeguarding policy. Pertinent points from the school eSafeguarding policy will be reinforced across the curriculum and across all subject areas when using ICT equipment within school.

The key messages contained within the eSafeguarding policy will be reflected and consistent within all acceptable use policies in place within school. The eSafeguarding policy will be introduced to the pupils at the start of each school year.

Roles and Responsibilities

We believe that eSafeguarding is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. More specific responsibilities and roles are detailed below:

- Senior Leadership Team: The executive headteacher and senior leadership team are responsible for ensuring that relevant staff receive suitable training to enable them to carry out their eSafeguarding roles and to train other colleagues when necessary. The executive headteacher and senior leadership team should also ensure that they are aware of procedures to be followed in the event of a serious eSafeguarding incident.

- eSafeguarding Coordinator: The eSafeguarding coordinator should promote an awareness and commitment to eSafeguarding throughout the school. They should also be the first point of contact in school on all eSafeguarding matters and should ensure that all staff are aware of the procedures that need to be followed in the event of an eSafeguarding incident. They should also communicate regularly with school technical staff.

- The responsibility of the eSafeguarding Governor is to ensure that the school eSafeguarding policy is current and pertinent, ensure that the school eSafeguarding policy is reviewed at prearranged time intervals and ensure that school Acceptable Use Policies are appropriate for the intended audience.

- Teachers and Support Staff: All staff should read, understand and help promote the school's eSafeguarding policies and guidance. Furthermore, they should read, understand and adhere to the school staff Acceptable Use Policy and report any suspected misuse or problem to the eSafeguarding coordinator, following the incident-reporting mechanisms that exist within the school. They should also develop and maintain an awareness of current eSafeguarding issues and guidance.

- Technical Staff: Technical staff should read, understand, contribute to and help promote the school's eSafeguarding policies and guidance. They must also report any eSafeguarding related issues that come to your attention to the eSafeguarding coordinator and support the school in providing a safe technical infrastructure to support learning and teaching.

- Pupils: Read, understand and adhere to the school pupil Acceptable Use Policy. Pupils should take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home. Furthermore, pupils should take responsibility for each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used outside school

- Parents and Carers: To help and support the school in promoting eSafeguarding and to read, understand and promote the school pupil Acceptable Use Policy with their children.

- Governing Body: To read, understand, contribute to and help promote the school's eSafeguarding policies and guidance. All safeguarding issues to be reported to K Sherburn and K Surtees.

- External Groups: The school will be sensitive and show empathy to internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice where appropriate. Where suitable, external groups will also be contacted for support or training relating to the safeguarding needs in our school, for example the PCSO. Managing Digital Content

Written permission from parents or carers will be obtained before photographs of pupils are published on Aston Lodge's website and others websites within the WPT. This information will be made available on the school website and in the school prospectus. We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound, as well as the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.

Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites.

Storage of Images

Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment. The school will store images of pupils that have left the school for 5 years following their departure for use in school activities and promotional resources. Staff have the responsibility of deleting the images when they are no longer required, or when a pupil has left the school.

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings. We aim to deliver this through a cross-curricular curriculum, and will incorporate eSafeguarding into appropriate areas of the curriculum.

ESafeguarding is embedded within our computing curriculum and PSHCE curriculum and is planned for within each year group in the school's long term planning. On the school long term plans it is evident that every year group will study eSafeguarding in ICT and at different depths according to year groups. Within the PSHE curriculum, e-Safeguarding is studied when learning about rights and responsibilities, bullying and its own stand of eSafety. Also, if specific eSafeguarding issues are raised, teachers should respond.

In order to ensure that we can deliver an appropriate, relevant and well balanced understanding of eSafeguarding, we will celebrate and promote eSafeguarding through a planned programme of assemblies and whole-school activities. Furthermore, we will discuss, remind or raise relevant

eSafeguarding messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials. Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.

Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way. We will remind pupils about their responsibilities through an end-user Acceptable Use Policy which every pupil will sign.

Our staff receive regular information and training on eSafeguarding issues in the form of staff meetings. Also, as part of the induction process, all new staff receive information and guidance on the eSafeguarding policy and the school's Acceptable Use Policies. All staff will be encouraged to incorporate eSafeguarding activities and awareness within their medium term planning, wherever it is appropriate.

Managing ICT systems and access

The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible. Servers, workstations and other hardware and software will be kept updated as appropriate. Virus protection is installed on all appropriate hardware, and will be kept active and up to date. All users will sign an end-user Acceptable Use Policy provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT systems and that such activity will be monitored and checked.

Passwords

Passwords are an important aspect of computer security. They are the front line of authentication for the protection of user accounts and their associated access to ICT equipment and resources. A poorly-chosen password may result in the compromise of a pupil's work, sensitive information regarding pupils or staff being lost or stolen, therefore it is crucial that a secure and robust username and password convention exists for all system access. As a staff we must lead the children by example, and illustrate the importance of passwords in order to protect their personal details and keep their technology safe.

Emerging Technologies

As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an eSafeguarding point of view. We will regularly amend the eSafeguarding policy (and computing policy) to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an eSafeguarding risk. Consequently, all new technologies will be tested and reviewed for any security vulnerabilities that may exist. Suitable countermeasures will be adopted within school to ensure that any risks are managed to an acceptable level.

Technology Matrix

Below is a table indicating the school's stance on use of digital devices during school hours for both adults and children.

	Staff and other adults				Pupils		
Communication technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Not allowed
Mobile phones may be brought to school	✓						✓
Use of mobile phones in lessons		✓ Via HT					✓
Use of mobile phones in social time	✓						✓
Taking photos on mobile phones or other camera devices				✓			✓
Use of handheld devices, e.g. PDAs, PSPs		✓				✓Treat days	
Use of blogs	✓					✓With adult	

Children who walk to and from school are allowed to bring a mobile phone into school which is left in reception first thing and collected at the end of school

Filtering Internet Access

The school uses a filtered internet service. The filtering system is provided by RGFL. The school will have a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.

Internet Access Authorisations

Parents will be asked to read the school Acceptable Use Policy for pupil access and discuss it with their children, when and where it is deemed appropriate. All pupils will have the appropriate awareness training and sign the pupil Acceptable Use Policy prior to being granted internet access within school. Furthermore, all staff will have the appropriate awareness training and sign the staff Acceptable Use Policy prior to being granted internet access within school.

All children will be closely supervised and monitored during their use of the internet. Pupils will be frequently reminded of internet safety issues and safe usage.

Email

Electronic mail (email) is an essential communication mechanism for both staff and pupils in today's digitally-connected world. The use of email can bring significant educational benefits for any school, both for its staff and pupils. Staff and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.

All email usage must directly correlate to the provisions detailed within the staff and pupil's acceptable use policies.

Publishing Content Online

We publish content online to enhance the curriculum by providing learning and teaching activities that allow pupils to publish their own content. However, we will ensure that staff and pupils take part in these activities in a safe and responsible manner. The content published is at the adult's discretion, but must model safe and responsible behaviour.

Mobile Phone Usage in School

Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times. All adults who enter the school premises during school time must be aware of this and must adhere to the school's stance. Pupils are not permitted to bring mobile phones into school. Rare, extenuating circumstances may be arranged between staff and parents whereby children may bring them into school, but they will be held by school staff at the owner's own risks. The school and staff do not take any responsibility for pupil's personal devices.

Staff will not use their mobile phones in class, unless for pre-arranged or emergency scenarios which must be pre-discussed with a member of the leadership team. Members of staff have no need to use personal devices within any school contexts; the school provides a communal mobile phone which can be used when on educational or residential visits. In emergency situations, staff may use their devices.

Data Protection and Information Security

The school has an up-to-date Data Protection Registration Certificate with the ICO (Information Commissions Office). All pupil data is recorded on the Capita SIMS Software and all office staff have access to pupil data through SIMS. Appropriate changes to children data, academic information, health issues etc. can only be made by the system manager. Parents are sent a questionnaire at the beginning of the Autumn term, each year, regarding data protection issues; particularly relating to the use of photographs of their children.

Specifically whether they can be:

- Included on the school website and other related WPT websites,
- Displayed in/around school, □ Released for publication to the press,
- Displayed in assessment folders,
- Released to DfE.

Parents will also be asked at the start of each year, in the Autumn term, whether they give permission for their details to be stored on Teachers2Parents, and if they wish to be contacted via this text messaging service.

Senior Information Risk Owner (SIRO)

The school has 'Senior Information Risk Owner' who is the head teacher.

Information Asset Owner (IAO)

The school has an 'Information Asset Owner' who is the school office manager. Their role is to understand:

- What information is held, and for what purposes,
- How information will be amended or added to over time,
- Who has access to the data and why,
- How information is retained and disposed of.

As a result the IAO manages and addresses risks to the information and makes sure that information handling complies with legal requirements.

Management and Assets

Details of all school-owned hardware will be recorded in a hardware inventory and details of all school-owned software will be recorded in a software inventory. All redundant ICT equipment will be disposed of through an authorised agency. It is the responsibility of all staff to log any equipment concerns in the ICT concern book to ensure that our equipment is both safe and fit for purpose.

Revised: January 2020