Heron Hill Primary School

ONLINE SAFETY POLICY and PROCEDURES

Approved by[1]	
Name:	Policy Review Committee
Signed:	
Date:	28 April 2021
Review date[2]:	April 2023

Designated Safeguarding Lead (DSL)	**Ian Murphy**
Online Safety/Safeguarding Link Governor	**Kirsty Turner**
PSHE/RSHE lead	**Rebecca Watson and Jenna Dollard**
Network Manager/other technical support	**Elite**
School IT Technician	**Alison Gorst**
Password Allocation	**Elite, Ian Murphy, Rebecca Watson**

ONLINE SAFETY POLICY

1. Background/Rationale

New technologies have become integral to the lives of children and young people in society, both within schools and in their lives outside school.

The Internet and other digital and information technologies are powerful tools, which open new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people have an entitlement to safe internet access.

The requirement to ensure that children and young people can use online and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The school Online Safety Policy and procedures will help to ensure safe and appropriate use. The development and implementation of such a strategy will involve all the stakeholders in a child's education from the Headteacher and Governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content;
- Unauthorised access to/loss of/sharing of personal information;
- The risk of being subject to grooming by those with whom they make contact on the internet;
- The risk of being targeted by extremists in order to promote and encourage radicalisation;
- The risk of being targeted by those involved in child sexual exploitation;
- The sharing/distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication/contact with others, including strangers;
- Cyberbullying;
- Access to unsuitable video/internet games;
- An inability to evaluate the quality, accuracy and relevance of information on the Internet;
- Plagiarism and copyright infringement;
- Illegal downloading of music or video files;
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this Online Safety Policy and procedures is used in conjunction with other school Policies including the Overarching Safeguarding Statement, Child Protection, Data Protection and Positive Behaviour and Discipline.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The Online Safety Policy and procedures that follows explains how we intend to do this, while also addressing wider educational issues to help young people (and their parents) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

2. Definitions

For the purposes of this document a child, young person, pupil or student is referred to as a 'child' or a 'pupil' and they are normally under 18 years of age.

Wherever the term 'parent' is used this includes any person with parental authority over the child concerned e.g. carers, legal guardians etc.

Wherever the term 'Headteacher' is used this also refers to any Senior Leader with the equivalent responsibility for children.

Wherever the term 'school' is used this also includes the Hive wrap around care.

3. Associated School Policies and Procedures

This Policy should be read in conjunction with the following school policies/procedures:

- Overarching Safeguarding Statement
- Child Protection Policy and procedures
- Data Protection Policy including procedures for CCTV
- Health and Safety Policy and procedures
- Positive Behaviour and Discipline Policy
- KCP Digital Image
- Whistleblowing procedures
- Code of Conduct for staff and other adults

4. Communication/Monitoring/Review of this Policy and Procedures

This policy and procedures will be communicated to staff, pupils and the wider community in the following ways:

- Posted on the school website/shared staff drive
- Policy and procedures to be discussed as part of the school induction pack for new staff and other relevant adults including (where relevant) the staff Acceptable Use Agreement
- Acceptable Use Agreements discussed with pupils at the start of each year
- Acceptable Use Agreements to be issued to external users of the school systems (e.g. Governors) usually on entry to the school
- Acceptable Use Agreements to be held in pupil and personnel files

The Online Safety Policy is referenced from within other school policies and procedures as outlined above. It replaces the school's E-Safety Policy.

The review period for this policy and procedures is as determined by the Governing Body and indicated on the front cover.

5. Scope of the Policy

This policy and procedures applies to all members of the school community (including staff, pupils, volunteers, parents, visitors, community users) who have access to and are users of our ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other online safety related incidents covered by this policy and procedures, which may take place out of school, but is linked to membership of the school. The 2011 Education Act increased these powers in relation to the searching for, and of, electronic devices and the deletion of data. In the case of both acts, action can only be taken in relation to issues covered by the published Positive Behaviour and Discipline Policy and procedures.

The school will deal with such incidents within this policy and procedures and the Positive Behaviour and Discipline Policy which includes anti-bullying procedures and will, where known, inform parents of incidents of inappropriate online safety behaviour that take place out of school.