OAKWORTH PRIMARY SCHOOL

"committed to the safety and welfare of its pupils"

E-SAFEGUARDING POLICY

E-Safeguarding Representatives

E-safeguarding Leads: Jess Clayton and Jenni Mayo (DSL)
E-safeguarding Governor: John Rogers
E-safeguarding Group: Jess Clayton (Computing Leader)
Matt Batey (IT technician)
John Rogers (Governor)

Aims

Oakworth Primary School is committed to safeguarding and promoting the welfare of all its pupils. We believe that:

- All children have the right to be protected from harm.
- Children need to be safe and feel safe in school;
- Children need support which matches their individual needs, including those who may have experienced abuse;
- All children have the right to speak freely and voice their values and beliefs;
- All children must be encouraged to respect each other's values and support each other;
- All children have the right to be supported to meet their emotional, social and educational needs – a happy, healthy, sociable child will achieve better educationally;
- Schools can and do contribute to the prevention of abuse, victimisation, bullying, exploitation, extreme behaviours, discriminatory views and risk taking behaviours;
- All staff and visitors have an important role to play in safeguarding children and protecting them from abuse.

Background Rationale

This policy will contribute to safeguarding our pupils and promote their welfare by:

- Clarifying standards of behaviour for staff and pupils;
- Contributing to the establishment of a safe, resilient and robust ethos in the school; built on mutual aspect, and shared values;
- Introducing appropriate work within the curriculum;
- Encouraging pupils and parents to participate;
- Alerting staff to the signs and indicators that might not be well;
- Developing staff awareness of the cause of abuse;
- Developing staffs' awareness of the risks and vulnerabilities their pupils face;
- Addressing concerns at the earliest possible stage;
- Reducing the potential risks pupils' face of being exposed to violence, extremism, exploitation or victimisation.

Expectations

All staff and visitors will:

- Be familiar with the Child Protection, Safeguarding and Prevent Duty policy.

- Be subject to safer recruitment processes and check, whether they are new staff, supply staff, contractors, volunteers etc.
- Be involved in the implementation of individual education programmes, integrated support plans, child in need plans and inter-agency child protection plans
- Be alert to signs and indicators of possible abuse
- Discuss concerns with the DSL (Jenni Mayo) or Deputy DSLs (James Travers, Danielle Blott, Sam Layfield and Paula Calvert)
- Deal with a disclosure of abuse from a child in line with the school's Safeguarding procedures.

Roles and Responsibilities

The Governing Body

Rev John Rogers is a member of the Governing Body and has been appointed the role of Safeguarding Governor (including E-safeguarding).

The Governing Body will ensure that:

- The school has a safeguarding policy, in accordance with statutory requirements.
- All staff who work with children regularly receive safeguarding training and updates (including E-safeguarding).
- Temporary staff and volunteers are made aware of the school's arrangements for child protection and their responsibilities.
- The school remedies any deficiencies or weaknesses in E-safeguarding brought to its attention, without delay.
- Forensic monitoring of online activity is in place.
- Termly reports are produced by the E-Safeguarding team (for the LGB).
- E-Safeguarding incidents and the school's response to these are logged on CPOMs.

The Headteacher (DSL)

- Jenni Mayo (Headteacher) is responsible the safety of members of the school community as the DSL, although actions directly relating to E-Safeguarding may be delegated to the Computing Lead, Jess Clayton..
- The Headteacher is responsible for ensuring that the Computing Leader and other relevant staff receive suitable CPD to enable them to carry out their E-Safeguarding roles and to train other colleagues, as relevant.
- The Headteacher and the Safeguarding Team should be aware of the procedures to be followed in the event of a serious E-Safeguarding allegation being made against a member of staff.
  - The Headteacher must have an up-to-date awareness of E-Safeguarding Matters
  - The Headteacher must also have an up-to-date awareness of the potential risk of serious child protection issues such as: sharing of personal information; access to illegal or inappropriate material; inappropriate contact with strangers; Potential / actual grooming; cyber-bullying; extremism/radicalisation.

E-Safeguarding Team

- Ensuring E-Safeguarding is a standing item on the computing group agenda.
- Annually reviewing the E-Safeguarding policy for the school.
- Providing training within the school community on E-Safeguarding.
- Meeting with the governor responsible for safeguarding on a termly basis.
- Liaising with the Local Authority
- Liaising with the School Computing Network.

- Logging all E-Safeguarding incidents on CPOMs, to help inform future E-Safeguarding practices and developments.
- Attending relevant meetings where appropriate
- Reporting regularly to the Senior Leadership Team.

ICT Technician

- Ensuring that the schools network is secure and not open to misuse or malicious attacks.
- Checking that the school is meeting E-Safeguarding technical requirements.
- Keeping at the forefront of E-Safeguarding technical information and keeping others informed as necessary.
- Ensuring that the school complies with statutory General Data Protection Requirements.

Education – Governor Training

- Governors should take part in regular E-Safeguarding training and awareness sessions. This may be delivered by members of the E-Safeguarding Group, School/Trust staff, external providers or through online units.

Teaching – Support Staff

- Having an up-to-date awareness of E-Safeguarding matters and the school policy, this also forms part of the induction process for new employees.
- Implementing the use of the Social Media and ICT Acceptable Use Policy
- Reporting any suspected misuse or problems to the school's ICT technician, DSL or E-safeguarding Team, for investigation.
- When using equipment, retiring to pupils of the school, E-Safeguarding policy/acceptable use policy and where there are breaches, reporting them to the E-Safeguarding Group, or member of staff.
- Ensuring that copyright law is abided by when using materials from the internet.
- Ensuring that computers are protected by an anti-virus solution (Sophos)

Education – Staff Training

It is essential that all staff receive E-Safeguarding training and understand their responsibilities, as outlined in this policy, training will be offered as follows;

- A staff meeting covering E-Safety will take place annually. This will be delivered by an external provider (eg. Izac Spencer-the school's link E-Safety PCSO)
- Online training through Sam Preston (Safeguarding Consultant).

Pupils

- Ensuring they use the school's ICT Systems appropriately following the schools E-Safeguarding policy and relevant Acceptable Use Policy Agreement (ie; the KS1 and KS2 Acceptable Use Policy Agreements are completed by all pupils and parents/carers on entry to the school).
- Having an understanding on how to report issues of abuse/misuse within the school.
- Knowing and following the school's policy on the use on personal electronic equipment
- Understanding the importance of good E-Safeguarding practise when using digital technology both inside and outside of the school environment
- Ensuring that copyright laws are explained and abided by

Parents and Carers

- The school will take every opportunity to help carers and parents to understand issues related to E-Safety. We will assist parents to understand key issues in the following ways;
  An annual parents' E-Safety information session, with a presentation; regular newsletters, offering parents advise on the use of the internet, gaming and social media sites at home.

- Parents will be asked to discuss the pupil Acceptable Use Policy with their children and are invited to sign a letter to say they done so.

- Ensuring their child understand the issues surrounding E-Safeguarding
- Endorsing the *Pupil Acceptable User Policy*. **Please note pupils will not be given access to the school network until the Acceptable Use Policy has been signed by both *pupil* and *parent/carer* and returned to the school office.**

Teaching and Learning

The purpose of the internet as a tool in school is to raise educational standards, promote pupil achievement, support the professional work of the staff and enhance the school's classroom learning experience.

Pupils at Oakworth Primary School are encouraged to use the internet both within and outside of school learning. It is important therefore to teach them the skills of using the internet appropriately, knowing and understanding the risks to allow them to take care of their own online security.

By allowing pupils and staff to use the internet, we are opening up a vast resource of information and materials to support their learning and continuing professional development. The School Internet access is designed expressly for pupils to use, and has a content management system provided by Bradford Council, which restricts certain key search words. Oakworth Primary School maintains a current record of all staff and pupils who are granted access on the school's network. All users must sign the *Acceptable Use Policy* before being allowed access to the school network, agreeing to comply with the E-Safeguarding rules. Parents/Carers will also be asked to sign a consent form for the pupil to be able to access the schools network, and being able to have access to the school's internet.

Pupils will be taught what the acceptable use of the ICT facilities is and given clear objectives for internet use. They will be made fully aware of the consequences of breaching these rules

The Prevent Duty

Since 2015, when the Government published the Prevent Strategy, there has been an awareness of the specific needs to safeguard children, young people and families from violent extremism. There have been several occasions nationally in which extremist groups have attempted to radicalise vulnerable people to hold extreme views including views justifying political, religious, sexist or racist violence, or to steer them into a rigid and narrow ideology that is intolerant of diversity and leaves them vulnerable to future radicalization. Oakworth Primary School is clear that this exploitation and radicalisation should be viewed as a safeguarding concern.

The school reduces the risk of radicalisation through its strong ethos, the promotion/celebration of British Values, the taught PSHE curriculum and activities that promote community cohesion. E-Safety teaching and learning also ensures that children know how to report any concerns and have strategies and knowledge to keep themselves safe online.

Social Media

All forms of social media sites will be blocked to pupils on roll. Training will be provided to ensure that all pupils are aware of the importance of not providing personal information that would allow another person to either identify them or their location. Advice will be given to pupils on acceptable practices when using social media sites outside of school. **Staff must NOT allow pupils to add them on social networking/media sites.**

The school will work with the relevant agencies to ensure that the systems to protect pupils are recovered and imported. If staff/pupils discover unsuitable sites these need to be reported to the ICT Technician and the E-Safeguarding Team.

New and upcoming technologies will be examined for educational benefit and a risk assessment carried out before being used within the school environment.

Use of Digital Media – Photographs, Video

- When using digital images, staff should inform and educate pupils about the risk associated with the taking, use and distribution of their own personal images online.
- Staff are allowed to take photos/videos to support educational learning and aims, Those images should only be taken on school equipment; the personal equipment of staff should not be used.
- Photographs of children published on websites should not contain names.
- Pupils' Full Names should **NOT** be used anywhere on websites or blogs.
- Written permission from parents or carers will be obtained before photographs of children are published on the school website.

Sexting

Making, possessing and distributing any imagery of someone under 18 which is 'indecent' is illegal. This includes imagery of a child sent by the child.

If an incident involving child produced sexual imagery comes to the school's attention:

The incident should be referred to the DSL as soon as possible.

- The DSL should hold an initial review meeting with appropriate school staff.
- There should be subsequent interviews with the children involved (if appropriate).
- Parents should be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm.
- At any point in the process, if there is a concern a young person has been harmed or is at risk of harm, a referral should be made to children's social care and/or the police immediately.

An initial review meeting should be held to consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people.
- If a referral should be made to the police and/or children's social care.
- If it is necessary to view the imagery in order to safeguard the child – in most cases, imagery should not be viewed.
- What further information is required to decide on the best response.
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services
- Any relevant facts about the young people involved which would influence risk assessment
- If there is a need to contact another school, college, setting or individual
- Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

An immediate referral to police and/or Children's Social Care should be made if at this initial stage:

1. The incident involves an adult.
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs).
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent.
4. The imagery involves sexual acts and any pupil in the imagery is under 13.

5. The school has reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming.

If none of the above apply, the school may decide to respond to the incident without involving the police or children's social care (the school can choose to escalate the incident at any time if further information/ concerns come to light). The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that she has enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and, if appropriate, local network of support.

School Information System

The security of the school's information system (SIMs) will be reviewed regularly and computers are to be protected with the school's antivirus solution. Any data stored will comply with GDPR legislation. Data that is required to be sent over the internet would be sent thought encrypted channels. Any files on the school network will be checked regularly for security purposes. Portable media (memory sticks, portable hard drives, CDs, etc.) may be used in the school, but only following a virus check to ensure that they are not infected. Staff do not take home any confidential data on portable media.

Email Accounts

All staff are given and expected to use a school Google email account, which will allow them to communicate with people outside school. It is up to the member of staff to ensure that all communication regarding the school is conducted in a professional manner and using only school systems.

Managing the Internet

The school provides pupils with supervised access to Internet resources through the school's fixed and mobile internet connectivity. Staff preview any recommended sites before use and raw image searches are discouraged when working with pupils. If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents are advised to supervise any further research.

Complaints of the internet misuse will be dealt with by the Headteacher and E-Safeguarding Team. Any complain about staff misuse must be reported directly to the Headteacher. Pupils, parents/carers and staff will be informed of the complaints procedure. It is expected that both pupils and parents/carers will work to support the school should any issues arise.

The consequences to pupils that will be implemented by Oakworth Primary School in the case of misuse may include parents/carers being informed and invited into school to discuss the situation.

The School Website

The contact details on the school's website include the schools address, phone/fax numbers and office email address, Staff and Pupil Personal Information should not be published. The Headteacher, ICT Technician, and PIW are responsible for ensuring that information on school's website, is correct, and provides a professional image of the school.

This policy will be reviewed every two years, or earlier if necessary.

Signed …….. 3 September 2018

Chair of Governors