Keeping Children Safe in Education (KCSiE) Policy

November 2016

Safeguarding

Bettridge School fully recognises its responsibilities for keeping children safe (Child Protection). Our policy applies to all staff (by staff, this means all staff employed by the school and volunteers) working in the school. There are five main elements to our policy:

1. Ensuring we practice safe recruitment in line with Government guidance by using at least one accredited recruiter on all interview panels, checking the suitability of staff and volunteers to work with children and ensuring any unsuitable behaviour is reported and managed using the Allegations Management procedures.
2. Raising awareness of Child Protection issues and equipping children with the skills needed to keep them safe.
3. Developing and implementing procedures for identifying and reporting cases (or suspected cases) of abuse by keeping up-to-date school records and referring to the Children's Helpdesk. Staff need to be aware of how to obtain **EARLY HELP** so that children receive the right help at the right time and co-ordinate with the relevant professionals.
4. Supporting pupils who have been or are subject to a Child Protection or Child in Need Plan.
5. Establishing a safe environment in which children can learn and develop.

We recognise that due to the day to day contact with children, school staff are well placed to observe the outward signs of abuse. The school will therefore:

- Establish and maintain an environment where children feel secure, are encouraged to talk, and are listened to.
- Ensure children know there are adults in the school who they can approach if they are worried.
- Include opportunities through the curriculum for children to develop the skills they need to recognise and stay safe from abuse and to express their feelings and concerns.

We will follow the procedures set out by the Gloucestershire Safeguarding Children's Board and take account of guidance issued by the Department for Children, Schools and Families to:

- Have a designated Safeguarding Lead for Safeguarding (DSL) (Child Protection) who has received appropriate training and support for this role. The Designated Safeguarding Lead is **Mandy Roberts** and Deputy Safeguarding Leads (DDSL) are **Jackie Hatton, Dale Hills and Jo Bunyan.** Have a nominated Governor

responsible for Child Protection who has received appropriate training. This is currently **Sue O'Gorman**.

- Ensure the DSL and DDSL are updated regularly, and at least annually to keep up with relevant developments in addition to undergoing relevant training every two years.
- Ensure all staff know they have a responsibility to safeguard all children and their families with whom they come into contact.
- Ensure all staff know the names of the designated Safeguarding Lead (DSL) responsible for child protection and their role.
- Ensure all staff understand their responsibilities in being alert to signs and responsibility for referring any concerns to the designated Safeguarding Lead responsible for child protection.
- Ensure all staff are aware of the signs of Radicalisation, Female Genital Mutilation (FGM) and Child Sexual Exploitation (CSE) and understand their responsibilities for referring any concerns to the designated Safeguarding Lead responsible for child protection.
- Ensure all staff are aware of the difference between a concern for a child (reported on a white Welfare Concern slip) and a situation where a child might be in immediate danger (Reported on a Yellow Welfare Concern slip and handing immediately to the DSL or a deputy DSL)
- Ensure all new staff read the 'Guidance for Safer Working Practices' document as part of the induction process. This is saved on the O:/General Information/School Policies and there is also a hardcopy book on the bookcase outside the Headteacher's office.
- Ensure all staff annually read the relevant KCSiE document and can answer key questions from it correctly to show understanding. A short induction covering the essentials of KCSiE will be given within the first week of employment using Gloucestershire Safeguarding Induction Pack for new staff.
- Provide training to include specific safeguarding issues: Child Sexual Exploitation (CSE), Bullying, Domestic Abuse, Drugs, Induced Illness, Female Genital Mutilation (FGM) and Forced Marriage.
- Ensure all staff have training in Safeguarding which is updated every three years. This will include learning from Serious Case Reviews both nationally and locally. New staff will complete the online training within 7 days of commencing employment.
- Ensure all staff have annual updates in Safeguarding. These can be delivered by the DSL or a deputy DSL
- Work closely with parents, pupils and professionals to keep children safe. In order to do this, the school makes available and shares relevant policies and documents with all stakeholders. Policies are on the website or can be given as hard copies if required.
- Notify the relevant social worker on the day if there is an unexplained absence of a pupil who has a Child Protection Plan.

- Develop effective links with relevant agencies and co-operate as required with their enquiries regarding Child Protection matters, including attendance at Child Protection conferences and core groups.
- Keep written records of concerns about children, even where there is no need to refer the matter immediately.
- Ensure all records are kept securely; separate from the main pupil file and in locked locations.
- Develop and follow local GSCB procedures where an allegation is made against a member of staff. Information can be found here: www.gscb.org.uk/handbook.

The school will endeavour to support the pupil through:

- Commitment to Pupil Voice activities and self-advocacy.
- Ensuring all pupils, staff and families are respected, whatever their gender identity, sexuality, ability, disability or family circumstances. No personal information should be discussed outside of the school without prior permission.
- Maintaining confidentiality in relation to the use of children's names, descriptions of their behaviour or learning disabilities and any other aspect that may be misinterpreted by those who do not understand such needs.
- The content of the curriculum.
- The school ethos which promotes a positive, supportive and secure environment and gives pupils a sense of being valued.
- Encouraging and developing self management of behaviour, which includes the use of safe spaces. All strategies are included in the Behaviour Policy and the Behaviour Management Physical Intervention Policy.
- Liaison with other agencies who support the pupil.
- Ensuring that, where a pupil who has a Child Protection Plan leaves, their information is transferred to the new school immediately and the child's Social Worker is informed.
- All visitors are provided with a 'Guidance for Visitors' booklet and sign to confirm they have read the safeguarding section.

E-Safety

Internet use is a part of the statutory curriculum and is a necessary tool for staff and pupils. Everyone in the school community has a personal responsibility to work towards keeping themselves and others safe online. School will not accept responsibility for any content that has not been accessed through the school network.

Infrastructure

- All aspects of the school IT systems are managed and reviewed by the IT Network & Development Manager. Internet access is a managed, filtered service provided through the South West Grid for Learning (SWGfL).
- Virus protection is purchased through our Microsoft Volume Licensing Agreement with SWGfL. Anti-Virus software is installed on all compatible school devices and updated regularly.
- Security strategies will be periodically discussed within the IT Core Working Party.
- Remote Access to the school network can, and will, only be initiated through 'school approved' and configured devices.
- Any school device that is taken off site which may contain school data is configured with centrally managed encryption.

Filtering

All internet access within school is filtered through the use of the standard filtering policies which are set by the SWGfL and custom filtering policies which are set by Bettridge School. These are designed specifically with safe pupil use in mind.

Where access to a specific website is required by staff but not students, the website is un-filtered via the SWGfL custom filtering policies and then filtered from pupil users through our pupil specific internal proxy server.

Staff Responsibilities

The IT Network & Development Manager regularly monitor internet access and brings any issues to the attention of the Leadership Team who then take appropriate action.

The IT Network & Development Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Staff or administrative users will protect the school from computer virus attack or technical disruption by not downloading from the internet any programs or executable files other than by agreement with the school's IT Network & Development Manager.

Staff will not procure goods or services direct over the internet except by specific agreement with the Headteacher/Business Manager.

Staff or approved adult school users should at all times abide by the copyright laws in respect of documents and materials downloaded from the internet.

Staff using a school laptop or other device off the school site, at home or elsewhere, still have to abide by this policy. Colleagues will be aware that the misuse of such devices for activity not agreed by the school may be breaking the law under the Computer Misuse Act 1990.

Staff must use a school supplied encrypted memory stick when taking any school data off-site.

Misuse and Complaints

Any E-Safety issues are logged and dated by the IT Network & Development Manager and any action taken is recorded. This includes information about the nature of the incident, who was involved and how it was dealt with. If the incident is of an illegal nature, the PC should be disconnected from the mains without shutting down first and the police and Local Authority Designated Officer (LADO) are informed. This log is reviewed to identify any trends in issues that may need addressing.

If staff or pupils discover an unsuitable site, it will be reported to the IT Network & Development Manager who will immediately ensure the website is filtered out and reported to the SWGfL.

Complaints of internet misuse will be dealt with by a member of the Leadership Team and any complaint about staff misuse will be referred to the Headteacher in accordance with the school's staff disciplinary procedures.

Login passwords must not be shared with anyone. Users are provided with their own login passwords which can be used to monitor any action taken when logged on and every user is responsible for the action taken while their username is in use.

Curriculum

Teaching

E-Safety is mapped into our PSHE (Personal Social Health Education)/PinK (People in the Know) curriculum. Pupils will be taught:

- About the need to keep their username and password private and not to share this information with anyone.
- What internet use is acceptable and what is not and given clear objectives for internet use.
- About the effective use of the internet in research, including the skills of knowledge, location, retrieval and evaluation.
- How to carry out internet searches in order to reduce the risk of accessing inappropriate material.
- About the effective and acceptable use of the internet for web publishing.
- To be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- About the safe use of the internet to support communications.
- About what to do if they encounter a problem and this includes how to report abuse.
- About what to do if they are bullied over the internet (Cyber or social media bullying).
- About their online presence and the importance of understanding permanence.

Managing Internet Access for Teaching

- Pupils will not carry out internet searches unless they have first been tested by a teacher/adult to ensure that they do not produce results containing inappropriate material.
- At Key Stage 1, access to the internet will be directly supervised to specific approved on-line materials.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, it is recognised that it is not possible to guarantee that unsuitable material will never appear on a school computer or on any pupils' personal device.

Training

- The IT Network & Development Manager will attend regular training in order to keep up-to-date with the latest recommendations.
- There will be regular briefings for staff. Staff will receive training on how to carry out internet searches safely and efficiently and how to minimise risk.
- The school will endeavour to ensure parents are supported in matters relating to E-Safety by sharing relevant information.
- School have two staff trained as CEOP (Child Exploitation and Online Protection) Ambassadors, who are available to support pupils, staff, parents and governors on E-safety.

Electronic Communications (e-mail and text)

- Pupils may only use approved e-mail on the school system.
- Pupils will be supported using e-mail and all staff should immediately tell a teacher/child protection officer if they or a pupil receive offensive e-mail or text. All pupil e-mails will be treated as public.
- Pupils must not reveal personal details of themselves or others in any online communication or arrange to meet anyone.
- Staff e-mails sent to an external organisation should be written carefully, in the same way as a letter would be written.
- The forwarding of chain messages is not permitted.
- Staff & pupils must be polite and considerate online and report any issues that are likely to cause offence to others.
- Teachers will agree with the class any timescales and responses to online messages and rules for collaborating online.
- Mobile phones (in any form) may not be used to take photographs/videos of any pupil at any time.

Social Networking and Personal Publishing

- The school will block/filter access to open social networking sites and give access only to those sites that are monitored and approved by SWGfL recommendations.
- Tools including message boards, blogs, instant messaging and collaboration tools will be used in this safer, closed environment.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be taught about the potential risks of social networking sites and what information should not be shared on such sites.
- Staff should not provide details or information of their own, or any other person or pupil that could relate to Bettridge School to internet sites including all social media, web blogs, forums or chat rooms e.g. Facebook, Twitter, etc. Exceptions should be checked with your line manager or Headteacher.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Acceptable Use of Video Conferencing and Skype

- Keep a log of all video conferences, including date, time and whom the conference was with and who else is present in the rooms.
- Children and young people must always be supervised by a member of staff when video conferencing with end-points beyond the school.
- Unsuitable content must be reported immediately to the Headteacher.

Voxer

- Clear guidelines about using Voxer are distributed to parents before they sign up to use the App. Staff must also read and follow the guidance.