Bilton Grange Internet and E-safety policy

Rationale

The internet and other digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning.

Aims

Our aims are to ensure that all pupils, including those with special educational needs:

- will use the internet and other digital technologies to support, extend and enhance their learning;
- will develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world including the need to avoid undesirable material;
- will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working;
- will use existing, as well as up and coming, technologies safely.

Internet use will support, extend and enhance learning

- Pupils will be given clear objectives for internet use.
- Web content will be subject to age-appropriate filters.
- Internet use will be embedded in the curriculum.

Pupils will develop an understanding of the uses, importance and limitations of the internet

- Pupils will be taught how to effectively use the internet for research purposes.
- Pupils will be taught to evaluate information on the internet.
- Pupils will be taught how to report inappropriate web content.
- Pupils will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working.
- Pupils will use the internet to enhance their learning experience.
- Pupils have opportunities to engage in independent and collaborative learning using the internet and other digital technologies.

Pupils will use existing technologies safely

- Pupils will be taught about e-safety through each unit of work in ICT lessons and other lessons involving the use of the internet.
- Discrete lessons on e-safety and cyber bullying will support this.

E-mail

- Staff will only use approved e-mail accounts when using the school network.
- Pupils will tell a member of staff if they receive inappropriate e-mail communications.
- Pupils will only use e-mail for approved activities.

Internet Access and Learning Platform

- Staff will read and sign the *NYCC Acceptable Use Policy.*
- Parents and children will read and sign Fronter Acceptable Use Policy so that they are aware of the rules of use of the internet in school including Fronter or any other applications that may be used by the school.
- Pupils will be taught to use the internet responsibly and to report any inappropriate content to a responsible adult.

Mobile Phones and other handheld technology

Pupils are only permitted to have mobile phones or other personal handheld technology in school with the permission of the Headteacher. When pupils are using mobile technology (their own or that provided by the school) they will be required to follow the school's Acceptable Use Policy (AUP). Such items can be confiscated by school staff if they have reason to think that they are being used to

compromise the wellbeing and safety of others (*Education and Inspections Act 2006, Sections 90, 91 and 94)*.

Web Filtering

- The school will work with Schools ICT to ensure that appropriate filtering is in place.
- Pupils will report any inappropriate content accessed to an appropriate member of staff.

Communication of the e-safety policy to pupils

- Pupils will read (or be read) and sign the age-appropriate Internet and Learning Platform Acceptable Use Policy before using these resources.
- Pupils will be informed that internet and Learning Platform use will be monitored.
- e-Safety will be included in the curriculum and regularly revisited

Communication of the e-safety policy to staff

- The e-safety and acceptable use policies will be given to all new members of staff as part of the staff handbook.
- The e-safety and acceptable use policies will be discussed with, and signed by, all staff.
- Staff will be informed that internet and Learning Platform use will be monitored.

Communication of the e-safety policy to parents/carers

- Parents will be asked to sign a home-school agreement when their children join the school. This will include acceptable use policies relating to the internet, Learning Platform and other digital technologies.
- The school will communicate and publicise e-safety issues to parents through the school newsletter, website and Learning Platform.

E-Safety Complaints

- Instances of pupil internet or Learning Platform misuse should be reported to a member of staff.
- Staff will be trained so they are able to deal with e-Safety incidents. They must log incidents reported to them and if necessary refer the matter to a senior member of staff.
- Instances of staff internet or Learning Platform misuse should be reported to, and will be dealt with by, the Headteacher.
- Pupils and parents will be informed of the consequences of internet and/or Learning Platform misuse.

Prevent Duty

- Prevent Duty is a multi-agency responsibility and those organisations providing services to children should have Prevent arrangements in place and work effectively with the Local Safeguarding Children Board.
- The aim of the Prevent strategy is to reduce the threat to the UK from terrorism by stopping people becoming terrorists or supporting terrorism. The Home Office oversees the Prevent strategy, which has 3 specific strategic objectives:
    1. Respond to the ideological challenge of terrorism and the threat faced from those who promote it;
    2. Prevent people from being drawn into terrorism and ensure they are given appropriate advice and support;
    3. Work with sectors and institutions where there are risks of radicalisation.

- The school will work to reduce the risk of exposure to radicalisation/extremism. The school will use the Prevent Duty Referral Protocol to guide the school when there is a Prevent referral (Appendix 1)

Key documents available are:

1. The DFE statutory guidance “Keeping children safe in education” 2015;
2. Working Together to Safeguard Children 2015;
3. Disqualification under the Childcare Act 2006 guidance 2015 ;
4. Channel Duty guidance 2015;
5. Channel: Vulnerability Assessment Framework 2012;
6. Prevent Duty guidance for England and Wales 2015; (there is separate guidance for Scotland);

7. Prevent Guidance, Ofsted 2015
8. Serious Crime Act 2015
9. Counter-Terrorism and Security Act 2015;
10. Counter-Extremism Strategy (HM Government, 2015)

Whole-School Responsibilities for Internet Safety

Headteacher

- Responsible for e-safety issues within the school but may delegate the day-to-day responsibility to a Senior Leader as the e-safety co-ordinator.
- Ensure that the e-safety co-ordinator is given appropriate time, support and authority to carry out their duties effectively.
- Ensure that developments at Local Authority level are communicated to the e-safety co-ordinator.
- Ensure that the Governing Body is informed of e-safety issues and policies.
- Ensure that appropriate funding is allocated to support e-safety activities throughout the school.

Governing Body

- Support the Headteacher in establishing and implementing policies, systems and procedures for ensuring a safe ICT learning environment.
- Ensure that appropriate funding is authorised for e-safety solutions, training and other activities as recommended by the Headteacher (as part of the wider remit of the Governing Body with regards to school budgets).
- Promote e-safety to parents and provide updates on e-safety policies within the statutory 'security' section of the annual report.

Network Manager/Technical Staff

- Provide a technical infrastructure to support e-safety practices.
- Ensure that appropriate processes and procedures are in place for responding to the discovery of illegal materials, or suspicion that such materials are, on the school's network.
- Ensure that appropriate processes and procedures are in place for responding to the discovery of inappropriate but legal materials on the school's network.
- Develop an understanding of relevant legislation.
- Report network breaches of acceptable use of ICT facilities to the Headteacher and/or the e-safety co-ordinator.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area.

Teaching and Support Staff

- Contribute to the development of e-safety policies.
- Adhere to acceptable use policies.
- Take responsibility for the security of data.
- Develop an awareness of e-safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.
- Include e-safety regularly in the curriculum.
- Deal with e-Safety issues they become aware of and know when and how to escalate incidents.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area.

Wider School Community

- This group includes: non-teaching staff; volunteers; student teachers; other adults using school internet, Learning Platform or other technologies.
- Contribute to the development of e-safety policies.
- Adhere to acceptable use policies.
- Take responsibility for the security of data.

- Develop an awareness of e-safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.
- Know when and how to escalate e-safety issues.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area.

Parents and Carers

- Read acceptable use policies and encourage their children to adhere to them.
- Adhere to acceptable use policies when using the school internet and/or Learning Platform.
- Discuss e-safety issues with their children, support the school in its e-safety approaches and reinforce appropriate behaviours at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Model appropriate uses of new and emerging technologies.
- Liase with the school if they suspect, or have identified, that their child is conducting risky behaviour online.

April 2016

To be updated April 2018

Appendix 1

PREVENT DUTY REFERRAL PROTOCOL

BILTON GRANGE PRIMARY SCHOOL PREVENT DUTY REFERRAL PROTOCOL

STEP 1	When a concern is identified, as with all safeguarding concerns, the member of staff may seek clarification from the individual but must be careful not to lead or investigate. Details of the concern are shared at the earliest opportunity with one of school's designated named persons for safeguarding. If using a computerised system, a safeguarding alert should be generated.
STEP 2	The designated named person for safeguarding will discuss the concern, including the relevant context with the member of staff (the referrer) and document the report. The member of staff will author, sign and date (including the time) a written statement for the safeguarding record in line with safeguarding recording requirements.
STEP 3	The designated named person for safeguarding to check if any additional concerns are known/documented in the school's safeguarding records then alert the Head Teacher or another designated named person. Jointly they should consider if the concern falls within general safeguarding concerns (see step 4) or if a Prevent referral should be made (see step 5). The named designated persons may wish to refer to *Channel Duty Guidance Protecting Young People from being drawn into terrorism* (p11,12) and *Channel: Vulnerability Framework* (p2,3) documents which contain guidance on vulnerability factors.
STEP 4	School to follow general safeguarding protocols taking action to support and/or make referral to social care where appropriate.
STEP 5	The designated named person for safeguarding to make a referral to the Local Authority safeguarding team. This is usually via the Local Safeguarding Children Board (LSCB) or the Multi-Agency Safeguarding Hub (MASH). However, some Local Authorities have designated a nominated Prevent referral lead within the authority to receive all Prevent referrals.