# The Brookfield School

# Online (E Safety) Protection Policy

## Introduction

Online/ e-safety may be described as the school's ability to:

- protect and educate pupils and staff in their use of technology
- have the appropriate mechanisms to intervene and support any incident where appropriate.

The breadth of issues classified within e-safety is considerable, but can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material
- contact: being subjected to harmful online interaction with other users
- conduct: personal online behaviour that increases the likelihood of, or causes, harm.

'Pupils with special educational needs are 16% more likely to be victims of online abuse.' (Ofsted, Inspecting e-safety 10 April 2014, No. 120196)

## Aims

The aim of technology used in school is to enhance teaching and learning and to enhance access to learning for pupils with sensory impairments, learning difficulties and/ or physical disabilities. This policy aims to minimise the risk to children and young people, to educate them about how to keep themselves online and to allow staff to intervene and support any incident where appropriate.

## Monitoring and Review

This policy has been developed by a working group made up of:

The Senior Leadership Team
Pupils (through student council)
Nominated staff members

Consultation with the whole school community has taken place through a range of formal and informal meetings. The policy will be monitored by the Headteacher and reviewed annually or more regularly in the light of any significant new developments in the use of the technologies, new threats online or incidents that have taken place.

## Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of academy IT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers the Headteacher 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 cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school but is linked to membership of the school.

The Brookfield School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

## Responsibility: Directors

Directors are responsible for the approval of the Policy and for reviewing the effectiveness of the policy. This will be carried out by the Safeguarding Director during regular meetings; Directors receive information about online incidents and monitoring reports during each Directors meeting.

## Responsibility: Senior Leadership Team

The Headteacher and Senior Leadership Team are aware of the procedures to be followed in the event of a serious allegation being made against a member of staff.
The School purchase software which provides safeguards against online abuse/ bullying:

Web filtering service
Antivirus software

## Responsibility: Designated/ Deputy Designated Safeguarding Leads

The named safeguarding leads in school are trained in issues and are aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data;
- access to illegal / inappropriate materials;
- inappropriate on-line contact with adults / strangers;
- potential or actual incidents of grooming;

- cyber-bullying.

**Responsibility: E-Safety Coordinator**

The Headteacher currently undertakes this role as part of the DSL role.

The e-Safety coordinator takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and acceptable use policies.

She ensures that all staff are aware of the procedures that need to be followed in the event of an incident taking place, provides training and advice for staff and liaises with the local authority and school technical staff through the SBM.

The e-Safety coordinator also receives reports of concerns and incidents and creates a log via an online recording system to inform future e-safety developments and training. She reviews incidents and issues regularly with the Senior Leadership Team and nominated Director. She ensures that technical staff regularly monitor network, email and internet access in order that any attempted misuse or misuse can be reported.

The SBM ensures that the school's technical staff manage IT systems so that they are secure, password protected and at an appropriate level for the user.

Staff and pupils have access to the drives through designated usernames and passwords. Sensitive documents will only be accessible to the relevant staff.

**Responsibility: Teachers and Support Staff**

All staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Senior Leadership Team, for investigation
- all digital communications with pupils or families should be on a professional level
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the online and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations where this is at an appropriate level
- they monitor the use of digital technologies, mobile devices, cameras etc. and implement current policies with regard to these devices where applicable
- in lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use. Staff are required to report anything that they deem as inappropriate to the SLT

## Education: Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of children and young people in online safety is therefore an essential part of the school's provision. Children and young people need the help and support of the school to recognise and avoid risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of the Computing / PHSE curricula and through activities led by the SLT and should be regularly revisited;
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities;
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT team can temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable i.e. written, with clear reasons for the need.

## Education: Parents

Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site,
- Parents / Carers sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. www.saferinternet.org.uk/ www.childnet.com/parents-and-carers

## Education: Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the training needs of all staff will be carried out regularly
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school policy and Acceptable Use Agreements
- The E-Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organizations and the Local Authority
- This e-safety policy and its updates will be presented to and discussed by staff in staff / team meetings or via INSET
- The E-Safety Coordinator will provide advice / guidance / training to individuals as required

## Education: Directors

Directors should take part in e-safety training / awareness sessions, with particular importance for the Director designated for Safeguarding and Child Protection.

This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in school training / information sessions for staff or parents.

## Technical Infrastructure

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements;
- There will be regular reviews and audits of the safety and security of school technical systems;
- Servers, wireless systems and cabling must be securely located and physical access restricted;
- All users will have clearly defined access rights to school technical systems and devices;
- Users are responsible for the security of their username and password;
- The administrator passwords for the school IT system, used by technician must also be available to the Headteacher or other nominated senior leader and kept in a secure place;
- The school technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations;
- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored;
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement;
- An appropriate system is in place for users to report any actual / potential technical incident / security breach via an online system (CPOMS).

## Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet.

However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. Once published they can also be downloaded by other individuals.

It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act).

Staff are allowed to take digital images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes unless in exceptional circumstances and with the permission of the Senior Leadership Team.

Care should be taken when taking digital images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Children and young people must not take, use, share, publish or distribute images of others without their permission.

Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

Pupils' full names will not be used anywhere on a website or blog in association with photographs.

Permission from parents or carers will be obtained before photographs of pupils are published on the school website or FaceBook site.

## Social Networking

Social networking is an everyday part of life for many of our children and young people, parents/ carers and staff.

Younger children are increasingly using social networking sites, as evidenced by the rise of usage by those aged 5–7 in the UK from 7% in 2009 to 23% in 2010. This is largely driven by sites aimed at young children such as Club Penguin and Moshi Monsters, rather than age-restricted sites like Facebook. However, Facebook remains enormously popular (96% of those aged 8–15 with an active social networking site profile use Facebook) and there are a significant number of underage users accessing sites like Facebook which have a minimum user age of 13 (from UK children's media literacy, Ofcom, 2011)

Social networking sites and MSN are blocked by the filtering service for schools so that they cannot be accessed on school premises. However, most children and young people access these sites from mobile devices. Staff are aware of the potential risks and will report any concerns to the Senior Leadership Team.

## Guidelines for Publishing on the School Website and Internet

On the school website, pupils work is displayed to show the work that pupils in different Key Stages have been completing. It is a powerful way to celebrate our children and young people's learning and achievement. When publishing pupils work on the internet, in any forum, we must consider the following:

- Give as little information about the child/ young person – it is better to refer to their key stage rather than age and the use of their first name only is recommended.
- Limit information to the activity depicted in photographs, give out no personal information about the child or young person.
- All staff and pupils should adhere to the applicable Acceptable Use Policy.
- Ensure that information is relevant and accurate.
- When publishing photographs of pupils engaged in sporting activities be cautious of what the photograph depicts. It is recommended that children and young people are not photographed in swimwear or minimal clothing.
- Take care publishing information that may make the school vulnerable to crime.
- When making and editing digital video, avoid referring to pupils by name (either use voice over or 'bleep out').
- If you use children and young people's names in credits, refer to first names only.

When publishing on the Internet, staff must be clear about the reason for publishing and who the target audience is. Materials on the internet are protected by copyright. If content is included in presentations, other work or to illustrate a page, then due recognition must be made of the source and permission must be sought for use.

Teachers may wish to use external websites or blogs created by themselves as part of their curriculum or to enhance learning. A link to these sites must be created from the school's website (located in the relevant area under 'Pupils') and a member of the Senior Leadership Team must be made aware of this to monitor content.

**Communications Technology**
**Own devices**

**Key Stage 2/3/4**

| | |
|---|---|
| Lesson Time/ Pastoral Time | No mobile phones.<br>AAC only, no other technology. |
| Breaks/ lunchtime | No mobile phones.<br>AAC only, no other technology. |

**This is to be discussed in School Council Autumn 2019.**

## Responding to Incidents of Misuse

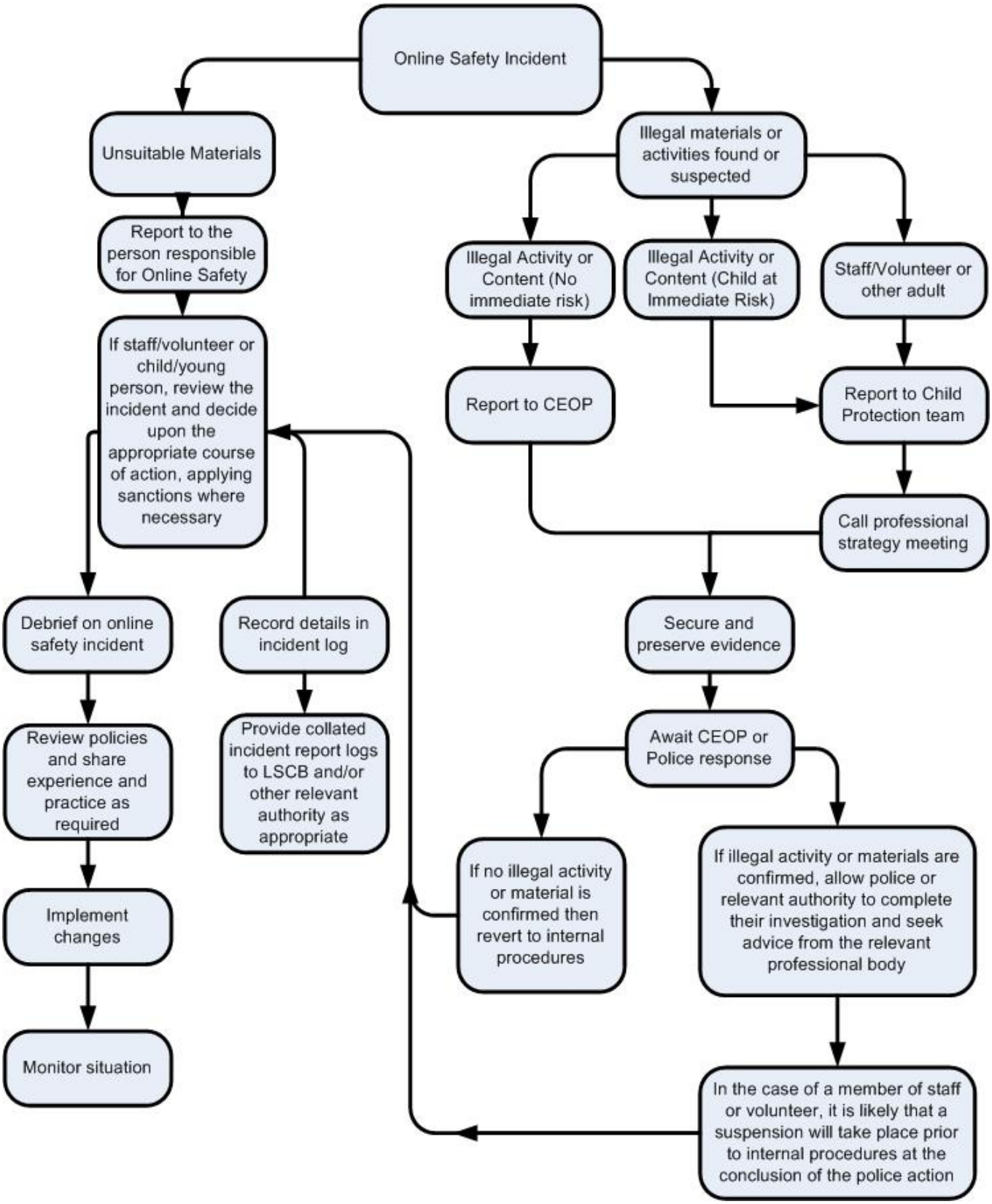
This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

## Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.

## Sanctions

All incidents which breach e-safety guidelines will be treated seriously and reported immediately. The actions taken will depend on the incident. Our aim is not to immediately sanction pupils but to educate and guide them towards future positive behaviour. Where a pupil displays frequent inappropriate use of a computer a behaviour plan and extra supervision will be put in places.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

## Web Links

Resources for Staff

http://www.northerngrid.org/resource/swurl (unblocking websites)

http://www.digitallyconfident.org/

https://www.e-safetysupport.com/

http://www.childnet.com/

http://www.lgfl.net/esafety/Pages/safeguarding.aspx

http://www.swgfl.org.uk/products-services/Online-Safety-Services

http://www.360safe.org.uk/Accreditation/E-Safety-Award

http://www.kelsi.org.uk/pupil_support_and_wellbeing/safety,_health_and_wellbeing/child_protection_safeguarding/e-safety.aspx

http://www.saferinternet.org.uk/

http://www.ofsted.gov.uk/sites/default/files/documents/inspection--forms-and-guides/i/Inspecting%20safeguarding%20in%20maintained%20schools%20and%20academies%20-%20a%20briefing%20for%20section%205%20inspections.pdf

Parents/ Carers and Staff

http://www.bbc.co.uk/webwise/0/

http://www.theparentzone.co.uk/parent

https://www.thinkuknow.co.uk/

http://www.kidsmart.org.uk/

http://www.childnet.com/

http://www.youtube.com/watch?v=d5kW4pI_VQw

http://www.safetynetkids.org.uk/personal-safety/staying-safe-online/