

# Baston House School

## Web Filtering Policy

### Schedule for Development/ Monitoring/ Review

<p>This web filtering policy was approved by the Board of Directors/ Governing Body / Governors Sub Committee on:</p>	<p>April 2018</p>
<p>The implementation of this web filtering policy will be monitored by the:</p>	<p>ICT / Online Safety Co-ordinator and the Senior Management Team</p>
<p>Monitoring review will take place at regular intervals:</p>	<p>At least bi-annually</p>
<p>Should serious online safety incidents take place, the following external persons / agencies should be informed:</p>	<p>(As appropriate) Multi Agency Safeguarding Hub (MASH) CEOP LADO Police</p>
<p>Should serious online safety incidents take place, the following Outcomes First Group colleagues must be informed:</p>	<p>Nicola Thomas, Group Head of Safeguarding</p>

## **1.0 Scope of the policy**

- 1.1** This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who access the internet over the school wireless network (e.g. a child using their own IT equipment at a residential school over the Wi-Fi is within scope, even though they have no access to school ICT systems).
- 1.2** Outcomes First Group places the safety of young people as its highest priority, including safeguarding children and young people when using digital technology. Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. However, Outcomes First Group takes its role seriously in ensuring that there are safe and secure systems in place.
- 1.3** The potential risks from internet use can be classified as:
- Content: being exposed to illegal, inappropriate or harmful material;
  - Contact: being subjected to harmful online interaction with other users; and
  - Conduct: personal online behaviour that increases the likelihood of, or causes, harm.
- 1.4** For this reason, Outcomes First Group operates a highly secure web filtering system on the internet link to the setting. This means that it safeguards the school's computers and internet use and it also offers safeguards on every mobile phone and tablet used in the setting over the setting's Wi-Fi network. Web filtering ensures that young people are safeguarded from illegal content and that they are protected from extremism online.
- 1.5** The web filtering system does not safeguard the use of a mobile phone or tablet that is accessing the internet over mobile phone signals. Controls on a young person's device to safeguard web browsing will need to be agreed between the young person, the school, the young person's parent or carer and their social worker. Staff must ensure a risk assessment is in place for any other device in use by children or young people in a school.
- 1.6** This policy should be read in conjunction with the individual setting's policies regarding safeguarding and child protection, online safety, and the use of mobile personal devices.
- 1.7** This policy is in line with the relevant Government legislation and guidance, including Keeping Children Safe in Education 2020. It will be reviewed whenever significant changes are made to national policy and legislation.

## **2.0 Roles and Responsibilities**

- 2.1** It is the responsibility of the school to ensure that all staff and visitors understand and implement this policy. It is the responsibility of the Head Teacher (Principal or Head of School) to ensure that staff comply with this policy and the accompanying, relevant policies.
- 2.2** It is the responsibility of the Head Teacher to ensure that online safety training for staff is aligned and integrated into the school's overall safeguarding training and approach.
- 2.3** All users should understand that the primary purpose of the use of the internet in a school context is educational. The web site categories that have been blocked are so as to ensure the safety and well-being of young people. However, it is accepted that on occasion some sites may need to be used as part of teaching such as regarding sex education, politics, religious education, and as part of personal, health and social educational lessons.
- 2.4** If a member of the teaching staff wishes to unblock a specific website either permanently or temporarily (for one day) to use within the classroom as part of learning this is to be discussed and verified by the school's ICT lead and the Designated Safeguarding Lead/Head Teacher. A record is to be kept by the Designated Safeguarding Lead of which sites are permanently unblocked and this is to be reviewed by them as part of the ongoing monitoring.
- 2.5** Lead ICT teachers and Designated Safeguarding Leads have the administration rights to temporarily unblock sites. The Designated Safeguarding Lead oversees the unblocking of sites. The Outcomes First Group IT Department has the administration rights to permanently unblock sites. No sites should be permanently unblocked by the Outcomes First Group IT Department without the written approval of the Group Head of Safeguarding or the Director of Quality and Outcomes. That written approval will be stored by the Outcomes First Group IT Department for future reference. The Group Head of Safeguarding will liaise with the Director of Quality and Outcomes as appropriate.
- 2.6** Blocked websites will be reviewed by Designated Safeguarding Leads with Head Teacher and Governors on a quarterly basis. Agreement to permanently unblock some sites at the request of the Designated Safeguarding Lead/Head Teacher/Governors can be reviewed prior to the formal quarterly review arrangements and in discussion with the Outcomes First Group IT Department and the Group Head of Safeguarding.
- 2.7** In line with Keeping Children Safe in Education 2020, internet use is monitored and reviewed. Reports setting out all internet use will be sent by the Outcomes First

Group IT Department to Designated Safeguarding Leads every six months. This information will be stored by the school for a period of six months unless there are safeguarding concerns. If there are safeguarding concerns the information will be stored in line with statutory requirements for record retention.

- 2.8** The social media website category is blocked within school hours (08:00-16:00) for staff and pupils. It is at the discretion of the Head Teacher and Head of Care if they allow pupils to use social media after school hours and as part of the residential care provided to young people. Staff are to ensure that they refer to the school's mobile devices policy.
- 2.9** Should attempts be made to access a site in the "child abuse" category then an immediate alert will be sent to the Designated Safeguarding Lead and the Head Teacher by Outcomes First Group IT Department. The website address and the device IP address it has been accessed from will be shared as part of this alert. This alert will also be sent to the Group Head of Safeguarding.
- 2.10** Attempts to access a blocked site in the categories "Extremist Groups", "Explicit Violence", "Pornography" and "Other adult materials" will be reported by the IT service provider to Outcomes First Group IT Department on a daily basis. IT will forward such reports to the Designated Safeguarding Lead and the Head Teacher, copying in the Group Head of Safeguarding. The website address and the device IP address it has been accessed from will be shared as part of this report.
- 2.11** Accessing of inappropriate sites must be investigated as possible safeguarding risks by the school Designated Safeguarding Lead.
- 2.12** The Designated Safeguarding Lead and Head Teacher are required to adhere to Outcomes First Group internal procedures relating to safeguarding and child protection and managing allegations as well as the schools Local Safeguarding Partnership's procedures.
- 2.13** Any accessing of websites related to extremism must be investigated and referred appropriately under Prevent duties by the school Designated Safeguarding Lead.
- 2.13** Breaches of this web filtering policy by staff will be considered a possible disciplinary offence.
- 3.0** Please see appendix (i) for the list of all blocked web site categories.

Author	Nicola Thomas
Document Title	Web Filtering Policy
Review Date	August 2021