

## NEWTON ROAD SCHOOL

### Academy Handbook: Policies and Procedures

Title	Online Safety
Associated Policies	<ul style="list-style-type: none"> <li>• Safeguarding and Child Protection</li> <li>• Special Educational Needs Policy</li> <li>• Academy staff code of conduct</li> <li>• Prevent and Radicalisation</li> <li>• Behaviour Policy</li> <li>• Data Protection Policy</li> <li>• Acceptable Use</li> <li>• Anti-bullying Policy</li> </ul>

**Reviewed:** September 2018

**Next Review:** September 2021

#### 1.0 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 school / academy digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of students / 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 online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The 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 Online Safety behaviour that take place out of school.

#### 2.0 Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

##### **Governors:**

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding governor which encompasses the role of Online-Safety governor). The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator / Officer
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / Board / Committee / meeting

##### **Principal and Senior Leaders:**

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.

- The Principal and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority / MAT / other relevant body disciplinary procedures).
- The Principal is responsible for ensuring that the Online Safety Officer / Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Officer / Lead.

### **Online Safety Lead – linked to Lead DSL role**

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority / MAT / relevant body
- Liaises with school technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- Meets regularly with Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs
- Reports regularly to Senior Leadership Team

### **Technical Staff:**

Because the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school technical staff. It is also important that the managed service provider is fully aware of the school / academy Online Safety Policy and procedures

The Network Manager / Technical Staff / Co-ordinator for ICT / Computing is responsible for ensuring:

- that the school’s technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority / MAT / other relevant body Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Learning Platform / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal and Online Safety Lead for investigation.
- that monitoring software / systems are implemented and updated as agreed in school / academy policies

### **Teaching and Support Staff**

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school / academy Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Principal or online safety lead for investigation
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the Online Safety Policy and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / 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

### **Designated Safeguarding Lead and Officers:**

Should be trained in Online Safety issues and be 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
- online-bullying

### **3.0 Education – Student/Pupils**

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety / digital literacy 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.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety 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 online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Students / 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.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. [N.b. additional duties for schools / academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.](#)

- Students / pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school / academy.
- 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 students / 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 students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

#### 4.0 Education – Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. 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 / academy will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
  - Letters, newsletters, web site,
  - Parents / Carers evenings / sessions
  - High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. [swgfl.org.uk](http://swgfl.org.uk)  
[www.saferinternet.org.uk/](http://www.saferinternet.org.uk/) <http://www.childnet.com/parents-and-carers>

#### 5.0 Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school / academy website will provide online safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online Safety provision

#### 6.0 Education & Training – Staff/Volunteers

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

- A planned programme of formal online safety training will be made available to staff.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school / academy Online Safety Policy and Acceptable Use Agreements.
- The Online Safety Officer / Lead (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.

- The Online Safety Officer / Lead (or other nominated person) will provide advice / guidance / training to individuals as required.

## 7.0 Training – Governors/Directors

Governors / Directors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety / safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / MAT / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in school / academy training / information sessions for staff or parents ([this may include attendance at assemblies / lessons](#)).