

# WEST DERBY SCHOOL



## ONLINE SAFETY POLICY

Approved on:	23/11/2016
Next review date:	Autumn term 2017
Signed:	S Graham (Headteacher)
Signed:	C Birch (For and on behalf of Governing Body)

West Derby School is a charitable company limited by guarantee, registered in England and Wales.

Company number 08166938. Registered office: 364 West Derby Road Liverpool L13 7HQ

## Schedule for Development/Monitoring/Review

This Online Safety policy has been developed by a working group made up of: Headteacher, Senior Leaders and Technical staff.

This Online Safety policy was approved by the Governing Body / Governors Sub Committee on:	23 <sup>rd</sup> November 2016
The implementation of this Online Safety policy will be monitored by:	The Safeguarding Team
Monitoring will take place at regular intervals:	Once a year
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	As per PWAG Governors Meetings
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	Autumn Term 2017
Should serious online safety incidents take place, the following external persons / agencies should be informed:	<ul style="list-style-type: none"> <li>• Paul Bradshaw, LA Senior School Improvement Officer</li> <li>• Police if necessary</li> </ul>
The school will monitor the impact of the policy using:	<ul style="list-style-type: none"> <li>• Logs of reported incidents</li> <li>• Monitoring logs of internet activity (including sites visited) / filtering</li> <li>• Internal monitoring data for network activity</li> <li>• Surveys / questionnaires of               <ul style="list-style-type: none"> <li>- students</li> <li>- parents / carers</li> </ul> </li> </ul>

## **Scope of the Policy**

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students 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 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.

## **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.

### **Headteacher and Senior Leaders:**

The Headteacher 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 Designated Safeguarding Lead.

The Headteacher and the Designated Safeguarding Lead are 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 HR / other relevant body disciplinary procedures). [Online Safety BOOST includes an ‘Incident Response Tool’ that outlines the steps \(and forms to complete\) any staff facing an issue, disclosure or report, need to follow. More information is available at: https://boost.swgfl.org.uk/](https://boost.swgfl.org.uk/)

The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. [Online Safety BOOST includes access to unlimited online webinar training – further details are at https://boost.swgfl.org.uk/](https://boost.swgfl.org.uk/)

The Senior Leadership Team will receive regular monitoring reports from the Designated Safeguarding Lead during the Safeguarding Team briefings.

### **Designated Safeguarding Lead:**

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- 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 / 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. [Online Safety BOOST includes access to Whisper, an anonymous reporting app that installs onto a school website and extends the schools ability to capture reports from staff, children and parents https://boost.swgfl.org.uk/](https://boost.swgfl.org.uk/)
- meets regularly with Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant committee of Governors
- reports regularly to Senior Leadership Team
- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

#### **Students:**

- are responsible for using the school digital technology systems in accordance with the Pupil Network and Internet Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

#### **Parents / Carers:**

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through the school. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website
- their children's personal devices in the school / school (where this is allowed)

#### **Policy Statements**

##### **Education – Students:**

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

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/ PSHCE/other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students 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 should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students 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.
- 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 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 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, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

#### **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 on-line 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 will therefore seek to provide information and awareness to parents and carers through:

- 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>

#### **Education & Training – Staff / Volunteers:**

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy.

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. [Online Safety BOOST includes unlimited online webinar training for all, or nominated, staff \(https://boost.swgfl.org.uk/\)](https://boost.swgfl.org.uk/)
- All new staff should receive online safety training as part of their induction

programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.

### **Training – Governors:**

**Governors 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 school / Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in school / school training / information sessions for staff or parents

### **Communications**

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

### **Social Media - Protecting Professional Identity**

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly, for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm are in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

**School staff should ensure that:**

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

**When official school social media accounts are established there is/are:**

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

**Personal Use:**

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

**Monitoring of Public Social Media**

The school's use of social media for professional purposes will be checked regularly by the Online Safety Officer to ensure compliance with the school policies.

**Use of digital and video images:**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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. 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 students 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.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website / social media / local press

## **Data Protection**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

## **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 Flowchart (below) for responding to online safety incidents and report immediately to the police.



