Online Safety Policy

This policy applies to EYFS as well as whole school

Owner	Head, Deputy Head and Head of Primary
Authorised by	Head and Governors
Dated	February 2018
Review	February 2019

Aims:

- **To ensure staff, students and parents understand the importance of on-line safety in school in relation to Safeguarding of young people**
- **To give clear guidelines about use of technologies in school**
- **To be clear about sanctions for misuse of technologies in school**

Learning

1. Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction.
- The school has a duty to provide pupils with high-quality Internet access as part of their learning experience.
- Internet use is a part of the curriculum and a necessary learning tool for staff and pupils.

2. Internet use will enhance and extend learning

- Staff will be made aware of and pupils will be educated in the safe use of the Internet.
- Clear boundaries will be set and discussed with staff and pupils, for the appropriate use of the Internet and digital communications.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

3. Pupils will be taught how to evaluate Internet content

- We will ensure that the use of internet-derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

1. Information system security

- The Derby High School ICT system security will be reviewed regularly.
- Virus protection will be installed and updated regularly.

2. E-mail

- All email communications between staff and students should be through school email accounts. School email accounts are monitored.
- Pupils must report any instance of abuse or misuse of the email to their form tutor or Head of Key Stage in the first instance. This includes any instance of offensive or inappropriate e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone, without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.
- A Bring Your Own Device (BYOD) network is provided for staff, Sixth Form students and guests, this networks internet access is filtered to the same KS5 level of any other computer on the network

3. Published content and the school website

- Staff or pupil personal contact information will not generally be published.
- Any contact details given online will direct communications to the school office.
- The Marketing Manager will have overall editorial responsibility for the website and will ensure that published content is accurate and appropriate.

4. Publishing students' images and work

- Photographs that include pupils will be selected carefully so that images of individual pupils cannot be misused, as far as it is possible to do so.
- Pupils' full names will not be used anywhere online, other than the password-protected areas on the school website, particularly in association with photographs.
- Written permission, using the approved permission form from parents or carers, will be obtained before photographs of pupils are published on the school website.

5. Social networking and personal publishing

- The school will educate staff in the safe use of social networking sites for their own protection, and will educate pupils in their safe use.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils will be made aware of how they can report abuse, including online, and to whom they should report abuse in school.
- Pupils will be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
- Pupils will be advised on security settings and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications.
- Pupils will be encouraged only to invite known friends and deny access to others.
- **Sexting** is a safeguarding issue. Even if explicit material is sent or elicited without malicious intent the consequences are serious and put those involved at risk of serious harm. Pupils are taught about sexting as part of their e-safety education. The School takes incidences of sexting extremely seriously, and deals with them in accordance with safeguarding procedures, including reporting to the police. (See Safeguarding Policy for further details.)

6. Managing monitoring and filtering

- In order to safeguard pupils and in line with the PREVENT strategy the school takes a robust approach to monitoring and filtering.
- The school will work to ensure that systems to protect pupils are reviewed and improved regularly.
- If staff or pupils discover an unsuitable site, it must be reported to the Senior Network Manager.
- The Senior Network Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Robust web filtering is built into Dell Sonicwall; this is based on a list of inappropriate websites which have been categorised by a third party. We can add websites to this list as we see fit.
- The filtering process looks for and blocks sites containing key words of concern e.g. Violence/ Hate/Racism/Illegal/Questionable Skills/Weapons.
- The Network Manager monitors the log file of the sonic wall list of issues/blocks. This means that: a) any repeated searching by a particular student would be noted, reported to the DSL and followed up and b) if there was an unprecedented failure of the filter, this would be picked up very quickly by the change in length of blocked searches.
- Students are monitored at random during un-supervised use of computers by the Network Manager; any behaviour of concern is reported to the Designated Safeguarding Lead. We force the use of “safe search” on search engines to filter out the worst of the web.
- All teachers have access to Impero which allows them to view the screens of students in their lesson.
- Students are aware of Impero and know that we can see what they are doing – Impero is used in lessons to demo students work via the teacher’s machine, a small thumbnail of every monitor is on the teacher’s screen so if a student was doing something wrong the teacher would see it.
- In line with the PREVENT strategy, if a student was identified as being at risk of being drawn into terrorism, their computer use would be closely monitored and access may be restricted.

7. Managing video-conferencing

- Video-conferencing will be set up with the advice of the Senior Network Manager with known organisations to ensure quality of service and appropriate security.
- Pupils should ask permission from the supervising teacher before making or answering a video-conference call.
- Video-conferencing will be appropriately supervised for the pupils’ ages.

8. Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The use of technologies such as mobile phones with wireless Internet access will be strictly monitored in school as they can bypass school filtering systems and present a new route to undesirable material and communications.

- Where contact with pupils is required to facilitate their learning, particularly on field trips or expeditions, staff will be issued with mobile phone numbers wherever possible.
- Mobile phones will not be used during lessons or formal school time, except where directed by the member of staff for educational reasons.
- The sending of abusive or inappropriate text messages/pictures is forbidden.
- The use by students of cameras in mobile phones will be kept under review.
- It is noted that games machines (including the Sony Playstation, Microsoft Xbox and others) have Internet access which may not include filtering. Care will be taken in any use in school or other officially sanctioned location.

9. Protecting personal data

- Any personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

1. Authorising Internet access

- All staff must read and agree to 'Staff Code of Conduct for ICT' before using any school ICT resource, including any laptop issued for professional use.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Key Stage 1 pupils: there will be an age appropriate level of explanation but pupils will not sign an agreement.
- Key Stage 2 pupils: the rules will be explained and the pupils will be expected to sign the 'Primary Computing Rules and On-line Safety Agreement'.
- Senior school pupils: the rules are explained and the pupils must sign the 'Secondary Computing Rules and On-line Safety Agreement'.
- Parents/carers will be provided with a copy of the relevant agreement.

2. Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network.
- The school cannot accept liability for any inappropriate material accessed, or any consequences of internet access.
- The school will audit ICT use to establish if the on-line safety policy is adequate and that the implementation of the on-line safety policy is appropriate and effective.
- The school will ensure the monitoring of software and that appropriate procedures are in place to highlight when action needs to be taken by the school.

3. Handling on-line safety complaints

- Complaints of Internet misuse will be reported to the Designated Safeguarding Lead in school and the Senior Network Manager. Action will be taken in line with Safeguarding as necessary.
- Any staff misuse that suggests a crime has been committed, a child has been harmed or that a member of staff is unsuitable to work with children will be reported to the LADO within one working day.
- Any complaint about staff misuse must be referred to the Headteacher and, if the misuse is by the Headteacher, it must be referred to the Chair of Governors.
- Pupils, parents and staff will be informed of the complaints procedure.
- Each case of misuse of technologies by a pupil will be considered separately and appropriate sanctions put in place. Permanent exclusion for the most serious cases, such as persistent bullying of another pupil, may result.

Communicating on-line safety

1. Introducing the on-line safety policy to pupils

- On-line Safety rules will be posted in all rooms where computers are used by pupils, appropriate to their age.
- All system users will be informed that network and internet use will be monitored.

- A programme of On-line Safety training and awareness raising is part of the school's commitment to promoting safe practices. This includes teaching through ICT and PSHE lessons, reinforcement across the curriculum, whenever appropriate, and use of assemblies to raise awareness and encourage responsible behaviour.

2. Staff and the On-line Safety policy

- All staff will be given access to the School On-line Safety Policy and its importance explained.
- Staff will be informed that network and Internet traffic can be monitored and traced to the individual user, including staff laptops.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior leadership and work to clear procedures for reporting issues.
- Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

3. Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School On-line Safety Policy in newsletters, the school brochure and on the school website.

Please refer to the following documents in conjunction with this policy:

- Staff Code of Conduct for ICT
- 'Computing Rules and On-line Safety Agreement - Primary'
- 'Computing Rules and On-line Safety Agreement - Seniors'
- Safeguarding policy
- PSHE policy

Please also refer to the Annual Audit document – last completed February 2018.