Online Safety Policy

Devoran School

Approved by:	Governing Body	**Date:**	19th October 2017
Last reviewed on:	19th October 2017		
Next review due by:	September 2018		

Aims and Objectives

Online safety encompasses the use of new technologies, internet, electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The online safety policy has been written by the school's ICT coordinator. It will be reviewed at least annually, with changes made immediately if technological or other developments so require.

Our policies and procedures, along with our daily systems and structures, reflect our strong ethos of 'no harm to others'. As part of Devoran School's commitment to online safety we fully support the Government's **Prevent Strategy**. Please refer to other school policies, in particular our Keeping Children Safe in Education safeguarding policy, as well as our Behaviour and Anti-Bullying policies.

Many of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites, pictures online or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour. It is the duty of the school to ensure that every child in our care is safe, and the same principles that we apply around the school's physical buildings should apply also to the 'virtual' or digital world.

There are 8 main areas of this policy:

1. Roles and responsibilities
2. Current technologies
3. Managing online safety risks
4. Strategies to minimise the risks
5. How will complaints regarding online safety be handled?
6. How will the policy be introduced to pupils?
7. How will the policy be discussed with staff?
8. How will parents' support be enlisted?
9. Online safety terminology

Roles and Responsibilities

Online safety is recognised as an essential aspect of strategic leadership in our school and the Headteacher, with the support of governors, aims to embed safe practices into the culture of the school. Our school's online safety coordinator will report to the Headteacher before taking any action.

Our online safety coordinator ensures they keep up to date with online safety issues and guidance through liaison with the Safeguarding Officer from the local governing body and through organisations such as the Child Exploitation and Online Protection (CEOP) organisation. The school's online safety coordinator ensures that the Headteacher, senior management team and governors are updated as necessary.

Governors need to have an overall understanding of online safety issues and strategies to minimise risks. We ensure our governors are aware of our local and national guidance on online safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school online safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

The following table details each group's various roles and responsibilities (but is not exhaustive):

Role	Key Responsibilities
Headteacher/ Deputy Headteachers	· To take overall responsibility for online safety provision · To take overall responsibility for data and data security · To ensure the school uses an approved, filtered internet service, which complies with current statutory requirements · To ensure that staff receive suitable training to carry out their online safety roles, and to train other colleagues as relevant · To be aware of procedures to be followed in the event of a serious online safety incident · To receive regular monitoring reports from the online safety coordinator · To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures (e.g. ICT technician/iCT4)
ICT Coordinator	· To take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school online safety policies/documents · To promote an awareness and commitment to e-safeguarding throughout the school community · To ensure that online safety education is embedded across the curriculum · To liaise with school ICT technical staff · To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident · To ensure that an online safety incident log is kept up to date · To facilitate training and advice for all staff · Is regularly updated in online safety issues and legislation, and aware of the potential for serious child protection issues to arise from: Sharing of personal data Access to illegal/inappropriate materials Inappropriate online contact with adults/strangers Potential or actual incidents of grooming Cyber-bullying and use of social media · To oversee the delivery of the online safety element of the computing curriculum
Governors	· To ensure that the school follows all current online safety advice to keep the children and staff safe · To approve the online safety policy and review its effectiveness · To support the school in encouraging parents and the wider community to become engaged in online safety activities

Network Manager/ICT Technician	· To report any online safety related issues that arise to the online safety coordinator · To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are changed every 90 days · To ensure that provision exists for misuse detection and malicious attack, e.g. keeping virus protection up to date · To ensure the security of the school ICT system · To ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices · To ensure that the school's policy on web filtering is applied and updated by iCT4 · To keep up-to-date with the school's online safety policy, as well as the latest technical information, to effectively carry out their online safety role and to inform and update others as relevant · To ensure that the use of network remote access/email is regularly monitored, so that any misuse or attempted misuse can be reported to the online safety coordinator/Headteacher for investigation/ action/sanction · To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster · To keep up-to-date documentation of the school's e-security and technical procedures
Teachers	· To embed online safety issues in all aspects of the curriculum and other school activities · To supervise and guide pupils carefully when engaged in learning activities involving online technology, including extracurricular and extended school activities where relevant · To ensure that pupils are fully aware of research skills · To ensure that pupils are fully aware of legal issues relating to electronic content, such as copyright laws
All Staff	· To read, understand and promote the school's online safety policies and guidance · To read, understand, sign and adhere to the school staff Acceptable Use Agreement · To be aware of online safety issues related to the use of mobile phones, cameras and hand-held devices, to monitor their use, and to implement current school policies with regard to these devices · To report any suspected misuse or problem to the online safety coordinator · To maintain an awareness of current online safety issues and guidance · To model safe, responsible and professional behaviours in their own use of technology · To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Pupils	· To abide by the Acceptable Use Agreement · To develop an understanding of research skills · To understand the need to avoid plagiarism and uphold copyright regulations · To understand the importance of reporting abuse, misuse or access to inappropriate materials · To know what action to take if they or someone they know feels worried or vulnerable when using online technology · To know and understand school policy on the use of mobile phones, digital cameras and hand-held devices · To know and understand school policy on the taking/using images and on cyber-bullying · To understand the importance of adopting good online safety practice when using digital technologies outside of school, and to realise that the school's online safety policy covers their actions outside of school when related to their membership of the school · To take responsibility for learning about the benefits and risks of using the internet and other technologies safely, both in school and at home · To help the school in the creation and review of online safety policies and the children's Acceptable Use Agreement
Parents/Carers	· To support the school in promoting online safety, and to endorse the parents' Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic images · To read, understand and promote the children's Acceptable Use Agreement with their children · To access the school website in accordance with the relevant school Acceptable Use Agreement · To consult with the school if they have any concerns about their children's use of technology

Current Technologies

Current technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include (with examples):

- The internet
- Email (Office 365, GMail)
- Instant messaging, often using phone cameras/webcams (FaceTime, Skype, Snapchat)
- Blogs
- Podcasts
- Social networking sites (Twitter, Facebook, Instagram, Club Penguin)
- Video broadcasting sites (YouTube)
- Chat rooms (TeenChat)
- Gaming sites (XBox/PlayStation online gaming, Neopets)
- Music download sites
- Mobile phones with camera and video functionality
- Mobile technology (e.g. applications on a device) that are 'internet ready'

- Smart phones with email, web functionality and cut-down 'Office' applications

Managing Online Safety Risks

Below are Devoran School's procedures regarding the following:

Internet access

1. The internet is an essential element of education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.
2. Internet use is a part of our curriculum and a necessary tool for staff and pupils.
3. The school internet access will be designed expressly for pupil use and will use an appropriate filtering system.
4. Pupils will be taught what internet use is acceptable and what is not, and will be given clear objectives for internet use. Pupils will not use the internet without having permission from a member of staff.
5. Pupils will have controlled access to social networking sites while in the school and will also be educated about the use of such sites safely in their own time.
6. Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
7. Pupils are forbidden from downloading games or other programs from the internet while at school.
8. The ICT technician will download programs from the internet as necessary.
9. Public chat-rooms and instant messaging are not allowed in school and are blocked by the internet filter.
10. Access to peer-to-peer networks is forbidden in the school (uTorrent etc.).
11. Pupils will be educated in 'Information Literacy' and taught how to evaluate internet content that they locate. Pupils will be taught the importance of cross-checking information before accepting its accuracy.
12. The school will ensure that the use of internet-derived materials by staff and pupils complies with copyright law. Pupils will be taught to reference materials that they have found from other sources so as not to infringe upon the intellectual property rights of others.
13. Pupils will be taught how to report unpleasant internet content.

Published content and the school website

14. Staff or pupils' personal contact information will not be published. The contact details given online should only refer to devoran.cornwall.sch.uk email addresses.
15. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
16. Permission from parents or carers will be obtained before photographs of pupils are published on the school website. Pupils' full names will not be used anywhere on the website or blog, particularly in association with photographs.
17. Work can only be published with the permission of the pupil and parents.
18. Pupil image file names will not refer to the pupil by name.
19. Pupil image files should be securely stored on the school network.

Video conferencing and webcam use

20. When available, video conferencing and webcam use will be appropriately supervised.
21. Only school-approved conferencing software will be used.
22. Pupils will be taught the dangers of using webcams outside of school.

Portable devices

23. Mobile phones are not to be used in the school; for children who walk home alone, mobile phones are to be left at the school office at the beginning of each day. The sending of abusive or inappropriate text messages may result in formal action being taken.
24. Staff should be aware that technologies such as ultra-portable laptops and mobile phones may provide access the internet, bypassing school filtering systems, and therefore present a new route to undesirable material and communications.
25. Staff should not use their personal mobile phones to contact pupils or capture photographs of children. Alternative equipment will be provided by the school.
26. Pupils will be taught how to protect themselves from being victims of theft and how to report such an event to the correct authority.

Managing emerging technologies

27. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the school is allowed.
28. Games consoles such as Sony PlayStation and Microsoft XBox provide internet access, which may not be filtered. Games consoles therefore may not be used in the school. The school's online safety strand within the computing curriculum ensures that every pupil is educated about the safe and responsible use of gaming consoles. Pupils are taught how to control and minimise online risks, and how to report a problem, through a range of activities that are flexible, relevant and engage pupils' interest.

Key Stage One includes the children being able to:

- recognise common uses of information technology **beyond school**
- use technology **safely and respectfully,** keeping personal information private
- identify where to go for **help and support** when they have concerns about **content or contact** on the internet or other online technologies
- understand what to do if they suffer from online peer-to-peer abuse through the use of the internet

Key Stage Two includes the children being able to:

- understand computer networks, including the internet; appreciate how they can provide multiple services, such as the world wide web; and recognise the opportunities that they offer for **communication and collaboration**
- use search technologies effectively, understanding how results are selected and ranked, and be **discerning in evaluating digital content**
- use technology **safely, respectfully and responsibly**; recognise **acceptable and unacceptable behaviour;** identify a range of ways to **report concerns about content and contact**
- understand what to do if they suffer from online peer-to-peer abuse through the use of the internet

How Will Complaints Regarding Online Safety be Handled?

The school will take all reasonable precautions to ensure the online safety of all pupils and staff. However, owing to the nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any other consequences of internet access.

Staff and pupils are given information about infringements and possible sanctions. Depending on the severity of the infringement, the response may be:

- An interview with the online safety coordinator or Headteacher;
- Informing parents or carers;
- Removal of internet or computer access for a period of time;
- Referral to the Police.

Our online safety coordinator acts as the first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying policy. Complaints related to child protection are dealt with in accordance with the school's child protection procedures.

How Will the Policy be Introduced to Pupils?

An all-day online safety training programme will take place once a year, to be delivered by a CEOP and Childline accredited organisation, for pupils, parents and staff, to raise the awareness and importance of safe and responsible internet use. This will be followed by termly reinforcement through staff workshops at staff meetings.

Online safety learning will be embedded and promoted across the curriculum and will form an important part of lessons that incorporate ICT, where regular online safety discussions will take place.

Throughout the academic year there will be explicit online safety assemblies delivered to pupils by staff to promote how to stay safe online.

Children will be taught online safety explicitly, at least once a week, in a cross-curricular lesson that involves the use of ICT during the five-minute online safety starter.

How Will the Policy be Discussed with Staff?

It is important that all staff feel confident to use new technologies in teaching. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies.

Staff must understand the rules for information systems misuse. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with the online safety coordinator to avoid any possible misunderstanding.

ICT use is widespread and all staff, including administration, governors and support staff should be included in appropriate awareness raising and training. Induction of new staff should include a discussion of the school's online safety policy.

How Will Parents' Support be Enlisted?

Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the internet. The school may be able to help parents plan appropriate, supervised use of the internet at home.

Internet issues will be handled sensitively and parents will be advised accordingly via online safety meetings, leaflets and relevant information on the school website.

A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home internet use.

Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents.

Online Safety Terminology

Acceptable Use Agreement: An agreement whereby a user agrees to abide by certain terms in order to gain access to a network or the internet. In the school context, it may also cover how other communications services, such as mobile phones, can be used on the school premises.

Avatar: A graphic identity selected by a user to represent themselves to the other parties in a chat-room or when using instant messaging.

Chat-Room: An area on the internet or other computer network where users can communicate in real time, often about a specific topic.

Filtering: A method used to prevent or block users' access to unsuitable material on the internet.

Information Literacy: The ability to locate pertinent information, evaluate its reliability, analyse and synthesise it to construct personal meaning and apply it to informed decision making.

Instant Messaging (IM): A type of communications service that enables you to create a kind of private chat room with another individual, or individuals, to communicate in real time over the internet. IM is analogous to a telephone 'conference call' with text-based, not voice-based, communication.

Peer-to-Peer (P2P): A peer-to-peer network allows users to directly access files and folders on each other's computers. Such file-sharing networks create weaknesses in network security by allowing outside users access to the school's resources.

Spam: Unsolicited junk email. The term is also used to describe junk text messages received via mobile phones. A related term, spim (or spIM), describes receiving spam via instant messaging.

Spoofing: Assuming the identity of someone else, using an email address either guessed or harvested from repositories of valid email addresses (such as the address book of a virus-infected computer). Spoofing is typically practised to veil the source of virus-laden emails or, often, to obtain sensitive information from spam recipients, without revealing the source of the spammer.

Trojan Horse: A virus which infects a computer by masquerading as a normal program. The program contains additional features added with malicious intent. Trojan horses have been known to activate webcams, for example, without the knowledge of the computer user.

Video Conferencing: The process of conducting a conference between two or more participants over a network, involving audio and text as well as video.

Virus: A computer program that enters a computer, often via email, and carries out a malicious act. A virus in a computer can corrupt or wipe all information in the hard drive,

including the system software. All users are advised to guard against this by installing anti-virus software.

Webcam: A camera connected to a computer that is connected to the internet. Webcams may be linked to internet websites, where visitors can see images from the webcam in real time, and may also be used for video calling via internet services such as FaceTime or Skype.