Downsway
Primary
School

Internet and E-Safety Policy

Date policy approved by Governing Board	**24/01/24**
Date of next review	**Jan 2027**
Policy owner	**SBM**
Policy on website Y/N	**Yes**
Compliance tracker updated Y/N	**Yes**

Downsway Primary School takes seriously its responsibility to protect and safeguard the welfare of children and young people in its care. “The welfare of the child is paramount” (Children Act 1989).

Our policy is built on the following five core principles:

1: Guided educational use

Internet usage on site should be for curricular educational benefits where Internet use includes accessing information online. The abilities to communicate widely and to publish easily are part of that curriculum and should form part of internet use. Curriculum Internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and well-managed Internet use will reduce the opportunities for activities that could be of little use or possibly dangerous.

2: Risk assessment

21st century life presents issues including violence, discrimination and exploitation from which staff, children and young people need to be protected. At the same time, the children must learn to recognise and avoid these risks – to become “Internet Wise”. Schools need to ensure that they are fully aware of the risks, performing risk assessments and implementing a policy for safe Internet use. Pupils need to know how to respond if/when they come across inappropriate material. Support can be found at www.thinkuknow.co.uk

Since pupils can obtain Internet access at home as well as in youth clubs, libraries, public access points and in homes, ideally a similar approach to risk assessment and Internet safety should be taken in all these locations, although risks do vary with the situation. Part of our education on online safety should equally be to influence safety in these locations through teaching the children how to keep safe online outside of schools.

3: Responsibility

Internet safety depends on staff, schools, governors, advisers, parents and the pupils themselves taking responsibility for the use of Internet and other communication technologies such as mobile phones. The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions must be judged carefully. There are a number of technical solutions to help limit Internet access. However, it is the appropriateness and consistency of the school’s e-safety policy that is of overriding importance.

4: Regulation

The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. In some cases, access within schools must simply be denied; for instance unmoderated chat rooms present immediate dangers and as such all chat rooms are usually banned. Fair rules, clarified by discussion and prominently displayed at the point of access will help pupils make responsible decisions.

5: Appropriate strategies

This document describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding pupils towards educational activities. Strategies must be selected to suit the school situation and their effectiveness monitored. ***There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.***

Our e-safety has been written by the school, building on government guidance. It has been agreed by the leadership team and approved by governors. It will be reviewed annually by the Subject Co-ordinator and presented to Governors and staff as appropriate.

Why is internet use important?

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Because the Internet is so widely available in an unmoderated form outside of school, providing a safe environment in school is vital to developing our pupils' ability to use this resource safely outside of school.

How will Internet use enhance learning?

- The school Internet access will be designed expressly for educational use and will include filtering appropriate to the age of pupils.
- Pupils will learn appropriate Internet use and be given clear objectives for Internet use.
- Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will also have the opportunity to explore communication online through strictly guided use of email or through self-publication (i.e. wikis, blogs, podcasts). These should be used as a means of presentation of curricular learning, enhancing the purposefulness of their learning.
- All current staff and pupils have Internet access. A log of all staff with unfiltered access to the Internet will be kept and reviewed regularly.
- Parents and pupils will complete and sign the Responsible Internet Use form and Consent for Use of Pupil Media form.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials.
- Parents will be informed that pupils will be provided with supervised Internet access.

How will filtering be managed?

- The SBM will review the popular permitted and banned sites accessed by the school every 6 months.
- The SBM will also take responsibility for the addition to or exclusion of sites on the filtering list. As such, there can be complete monitoring of which websites are allowed or blocked at any time.
- Requests for sites to be added or removed from the block list should be taken to the SBM, preferably by email unless of an urgent nature.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the SBM.
- The school will work in partnership with parents, West Berkshire Council, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

How will the risks be assessed?

- Some material available via the Internet will be illegal or in other ways unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the current nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor West Berkshire Council can accept liability for the material accessed, or any consequences of Internet access.
- Should a site lead to the appearance of inappropriate or illegal material, the user should report the URL to the SBM as above.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Headteacher and SBM will ensure that the Internet policy is implemented and compliance with the policy monitored.

Managing Content

- As above, if staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the SBM who will then report it to the Internet Service Provider.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Specific lessons will be included within the Computing Scheme of Work that teaches all pupils how to research information from web resources.
- As above, the SBM will be responsible for permitting and denying additional websites as requested by colleagues.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How should website content be managed?

- The point of contact on the website will be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Website photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. We will also ensure that no clashes occur with child protection information; no photos are to be used on the website if parents have withheld permission for photos to be taken of their child(ren)
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Where audio and video are included (e.g. Podcasts, Video Blogging or embedded YouTube, Vimeo, etc clips) the nature of the items uploaded will not include content that allows the pupils to be identified. If embedded clips are used, the source page that can be accessed must also be checked to ensure no identification of pupils can occur.
- The Governing Board will take overall editorial responsibility for the school website. They will ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Communication – Managing e-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.
- Pupils should use email in an acceptable way. Sending images without consent and messages that cause distress and harassment to others, are considered significant breaches of school conduct and will be dealt with accordingly.
- Pupil access (in school) to external personal e-mail accounts will be blocked. However, staff will have access to personal email accounts in order to access information needed at school.
- Staff e-mail use during school hours should be restricted to education use when on site. That said, there may be times when staff need to use e-mail at lunch or before/after school and this is to be accepted on the basis that e-mail use is appropriate at school (see acceptable internet use above).
- Pupil e-mails, sent to an external organisation, should be written carefully and authorised by the teacher before sending, in the same way as a letter written on school headed paper.

On-line communications and social networking.

- Pupils will be taught about how to keep personal information safe when using online services. Each year group will have specific Computing lessons dedicated to e-safety.

- The school will conduct pupil surveys about home use of ICT. It will gauge the range of activities which pupils undertake and how safely they are using them, e.g. keeping personal information safe, experiences of cyber bullying etc.
- The use of online chat is not permitted in school.
- Access to social networks will be blocked at school for pupils.
- Although these sites require users to be above primary age, we must accept that by the end of KS2 many children will have accounts regardless. As such, we have some responsibility to incorporate education on safe usage of social networks in e-safety education.
- Staff are responsible for their Facebook (and other social networking) pages, and should take steps to ensure that all content is kept private. It is recommended that staff assess the security of their social network profiles every 6 months to ensure they continue to remain private.
- Social network profiles should also be representative of the professional nature of working in schools, and, as far as possible, staff should try to maintain a professional appearance even if their profile is private.
- It is best practice for staff not to add parents to any social networks as this can lead to inappropriate communication or accidental publication of sensitive information across parent body.
- In accordance with child protection policies, no staff may add pupils to any social networks (including seemingly safe ones such as XBoxLive or PSN) at any time. Staff may not disclose social network details to pupils that could lead to pupil's actively searching for them.
- Pupils may not search for staff online, and if any pupils attempt to add staff, this must be reported to the SBM and the Headteacher as soon as possible. The pupil should be blocked and no communication should be entered into online at all. Staff should exercise extreme caution in online dealings with other users whose identity they do not know since pupils may use online pseudonyms.
- Pupils attempting to find staff should be considered in breach of the home-school agreement and should be treated accordingly.

Mobile technologies

- Mobile phones are not permitted within the school. Pupils will be asked to give them to the school office at the start of the school day for safe keeping.
- Technologies such as Smartwatches, which have similar functions to mobile phones, e.g. internet or call capabilities, cameras etc., are not permitted to be worn in school.
- Mobile phones can access the internet via 3/4/5G communications. As such, any pupil with a mobile phone has unlimited access to the internet at any time. Consequently, mobile phones may not be in the possession of pupils at any time during any educational activities.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Introducing the Policy to Pupils

- Rules for Internet access will be posted in each classroom.
- A module on responsible Internet use and e-safety will be included in the curriculum covering both school and home use. This will include the necessity of keeping personal information safe, how to use mobile technologies appropriately and using online communication appropriately.
- Instruction on responsible and safe use should precede Internet access.
- Pupils will be informed that Internet use will be monitored.

Parents and E-Safety

- Parents' attention will be drawn to the school's E-Safety Policy on the school website at the beginning of a pupil's school life
- Information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Interested parents will be referred to organisations such as those listed in the reference section of this document.
- All parents will receive support information as and when available.

Consulting with Staff and their inclusion in the E-safety Policy

Any groups using the school's ICT facilities, and in particular the Internet, should sign a copy of the acceptable use policy before being provided with access. Internet use should be included in the induction of new staff.

- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained.
- The school's consequences for Internet and mobile phone / Personal Digital Assistants / technology misuse will be clear so that all teachers are confident to apply this should the situation arise.
- All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.
- Staff should be aware that Internet traffic is monitored and reported by the Internet Service Provider and can be traced to the individual user. Discretion and professional conduct is essential.
- Community users of the school's ICT facilities must sign the acceptable user policy before being granted access.
- Staff development in safe and responsible Internet use and on the school Internet policy will be provided as required.

How will complaints be handled?

- Responsibility for handling incidents will be delegated to the Headteacher.
- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- As with drugs issues, there may be occasions when the police must be contacted. early contact could be made to establish the legal position and discuss strategies.
- Sanctions available include:
  - interview/counselling by Headteacher.
  - informing parents or carers.
  - pupils being restricted from online access.

Linked Policies
Taking and storing images of children policy
Child Protection and Safeguarding policy

Date Reviewed	24th January 2024
Date of Next Review	January 2027

Responsible Internet Use

These rules help us to be fair to others and keep everyone safe.

- I will ask permission before using the Internet.
- I will use only my class network login and password, which is secret.
- I will only open or delete my own files.
- I understand that I must not bring into school and use software or files unless authorised by my teacher.
- I will only e-mail and open attachments from people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- I understand that I must never give my home address or phone number, or arrange to meet someone.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I understand that the school may check my computer files, e-mails I send and the Internet sites I visit.
- I will respect copyright rules when I am on the internet.
- I will never search for staff on social networks (even at home) and understand that I will be reported to the Headteacher by staff if I do.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.
- The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
- Our Internet Service Provider monitors all Internet use and will notify the police and Local Authority if an illegal website is accessed.

Dear Parents/Carers

Responsible Internet Use

As part of your child's curriculum and the development of Computing skills, Downsway Primary School provides supervised and restricted access to the Internet. We believe that the effective use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached Rules for Responsible Internet Use and sign and return the consent form so that your child may use the Internet at school.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The school will not be liable for any damages arising from your child's use of the Internet facilities.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school Internet provider, operates a filtering system that restricts access to inappropriate materials. Children are also taught about responsible use of the internet and are taught to search online in a manner that will reduce the likelihood of discovering unwanted results.

We recommend you read our Internet & E-Safety policy, which can be found on our school website, prior to your child starting at Downsway.

Should you wish to discuss any aspect of Internet use or how to keep safe online, please contact the school office for an appointment.

Yours sincerely

Headteacher

Downsway Primary School
Responsible Internet Use

Please complete, sign and return to the school office

Pupil:	***Class:***

Pupil’s Agreement

I have read and I understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and follow these rules at all times.

Signed:	***Date:***

Parent’s Consent for Internet Access

I have read and understood the school rules for responsible Internet use and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	***Date:***

Please print name:

Parent’s Consent for Web Publication of Work and Photographs

I agree that, if selected, my son/daughter’s work may be published on the school Website. I also agree that images, sound files and video that include my son/daughter may be published subject to the school rules that this content will not clearly identify individuals and that full names will not be used.

Signed:	***Date:***

Downsway Primary School

Consent form for taking and using photos and videos

Child's name: ………………………………………………………………………..

Dear Parent/Carer,

At Downsway School, we sometimes take photographs/videos of pupils. We may use these photos/videos in the school's prospectus, on the school's website, in newsletters and on display boards around school. We may also make video or webcam recordings for school to school conferences, monitoring or to record school productions. At times, we are visited by the media who may take photographs or videos for use in local or national newspapers or on televised news programmes.

We really value using photos and videos of pupils, to be able to showcase what pupils do in school and show what life at our school is like to others, so we would appreciate you taking the time to complete this form. We would like your consent to take photos and videos of your child, and use them in the ways described above. If you're not happy for us to do this, that's no problem – we will accommodate your preferences.

Please tick the relevant box(es) below and return this form to school.

I am happy for the school to take photographs of my child.
Our current photographers are Lisa Plevey and Tempest. □

I am happy for photos/videos of my child to be used on the school website. □

I am happy for photos of my child to be used in the school newsletter. □

I am happy for photos of my child to be used in the school prospectus. □

I am happy for photos of my child to be used in internal displays. □

I am happy for videos of my child to be used for school-to-school conferences. □

I am happy for photos/videos of my child to be used for assessment purposes, e.g. children's books, journals, SeeSaws etc. □

I am happy for photos/videos of my child to be taken in school productions. □

I am happy for photos/videos of my child to be taken by the media for use in newspapers or television. □

I am happy for photos/videos of my child to be used on social media, including the Downsway's Facebook page. □

I am **NOT** happy for the school to take or use photos or videos of my child. □

If you change your mind at any time, you can let us know by emailing office@downsway.w-berks.sch.uk, calling the school on 0118 9421362 or just popping into the school office. If you have any other questions, please get in touch.

Parent/Carer's signature: ……………………………………… Date ………………………

Downsway Primary School

Laptop Policy

1. The laptop remains the property of Downsway School.
2. The laptop is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated. Only Downsway School staff should use the laptop.
3. On the teacher leaving the school's employment, the laptop is returned to Downsway School. Staff on extended leave of 4 weeks and over should return their laptops to the school (other than by prior agreement with the Headteacher).
4. When in school and not being used, the laptop must be kept in a safe and secure place. It must not be left in an unlocked, unattended classroom outside of school hours.
5. Whenever possible, the laptop must not be left in an unattended car. If there is a need to do so it should be locked in the boot.
6. The laptop must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the Headteacher with evidence of adequate insurance.
7. The school has a higher policy excess than the value of the laptop, so in the event of a loss which results from these guidelines not being followed, it is unlikely that the school will cover the cost of replacement from centrally held funds and, depending on the circumstances, you may be considered liable. If the laptop is stolen from an un-attended car, you will be responsible for its replacement in any event. You are strongly urged to cover the laptop under your home insurance, the value being £500.
8. Staff may load their own software onto the laptop but it must be legal, fully licensed and not corrupt any software or systems already installed on the laptop. Staff are responsible for ensuring software is virus-free.
9. Anti-virus software is installed and must be updated on a weekly basis.
10. As the administrator password is required to install software, staff will need to report to the SBM or ICT co-ordinator to do this. Please begin the installation until a password is required, then bring your laptop to a member of staff with administrator privileges.
11. Any software installed must not affect the integrity of the school network.
12. If any removable media (USB sticks, etc.) are used then it must be checked to ensure it is free from any viruses.
13. It will be the responsibility of the member of staff to ensure that the virus protection software that has been installed on the laptop is kept up-to-date.
14. Staff must use their laptop in school on the network at least once a week to ensure virus protection is automatically updated.
15. Staff should not attempt to significantly alter the computer settings other than to personalise their desktop working area.
16. Students must never use the laptop.
17. If any fault occurs with the laptop, it should be referred immediately to the SBM who can get in touch with companies responsible for maintenance. If the fault looks as though it could be easily fixed, report it to the SBM who may be able to solve the issue without cost to the school. Under no circumstances should staff attempt to fix suspected hardware faults.
18. When being transported, the carrying case supplied must be used at all times.
19. The laptop would be covered by normal household insurance, if not it should be kept in school and locked up overnight.

Laptop make …………………….. Model ……………………………. Serial No. ……………………

Authorised by Headteacher …………………………………………….. Date …………………………

Member of staff ……………………………………………………………

Received (signature) ………………………………………………….. Date ………………………….

Downsway Primary School

Staff policy for responsible e-mail, network and Internet use

1. I will use all ICT equipment issued to me in an appropriate way. I will not:
   - Access offensive websites or download offensive material.
   - Make excessive personal use of the Internet or e-mail.
   - Copy information from the Internet that is copyright or without the owner's permission.
   - Place inappropriate material onto the Internet.
   - Send e-mails that are offensive or otherwise inappropriate.
   - Disregard my responsibilities for security and confidentiality.
   - Download files that will adversely affect the security of the laptop and school network.
   - Access the files of others or attempt to significantly alter the computer settings.
   - Update web pages etc. or use pictures or text that can identify the school, without the permission of the Headteacher. This also applies at home.
   - Make any attempt to repair or interfere with the components, software or peripherals of any computer that is the property of Downsway School unless I know exactly what I am doing. If I am not competent to do this, I will report faults as per point 17 on the laptop policy above.
2. I will only access the system with my own name and registered password, which I will keep secret.
3. I will inform the SBM as soon as possible if I know my password is no longer secret.
4. I will always log off the system when I have finished working.
5. I understand that the school may, in line with policy, check my computer files and school e-mails and may also monitor the Internet sites I visit.
6. My files should not, routinely, be password protected by my own passwords. Should a confidential matter warrant this, I must gain permission from the Headteacher and register the passwords with the Headteacher.
7. If I use removable media, I will ensure that this has been carefully checked to ensure it is free from any type of virus.
8. I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the SBM.
9. All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be used.
10. School e-mail usage should be for educational benefit and private emails between colleagues of a non-school nature should be sent to and from private addresses outside of school hours.
11. I will report immediately to the Headteacher any unpleasant material or messages sent to me.
12. I understand that a criminal offence may be committed by deliberately accessing Internet sites that contain certain illegal material.
13. Use for personal financial gain, gambling, political purposes or advertising or any illegal purpose is forbidden.
14. Storage of e-mails and attachments should be minimised to avoid filling the limit available – no further emails can be received once this limit is reached.
15. Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
16. I understand that if I do not adhere to these rules, my network access will be suspended immediately, my laptop removed and that other disciplinary consequences may follow.

Name...

Signature: ....

Date: ....

Information and support

There is a wealth of information available to support schools, colleges and parents/carers to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Advice for governing bodies/proprietors and senior leaders

- Childnet provide guidance for schools on cyberbullying

- Educateagainsthate provides practical advice and support on protecting children
from extremism and radicalisation

- London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements

- NSPCC provides advice on all aspects of a school or college's online safety Arrangements

- Safer recruitment consortium "guidance for safe working practice", which may help
ensure staff behaviour policies are robust and effective

- Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones

- South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements

- Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq

- UK Council for Internet Safety have provided advice on sexting-in-schools-and colleges and using-external-visitors-to-support-online-safety-education

Remote education, virtual lessons and live streaming

- Case studies on remote education practice are available for schools to learn from
each other

- Departmental guidance on safeguarding and remote education including planning
remote education strategies and teaching remotely

- London Grid for Learning guidance, including platform specific advice

- National cyber security centre guidance on choosing, configuring and deploying video conferencing

- National cyber security centre guidance on how to set up and use video Conferencing

- UK Safer Internet Centre guidance on safe remote learning

Support for children

- Childline for free and confidential advice

- UK Safer Internet Centre to report and remove harmful online content

- CEOP for advice on making a report about online abuse

Parental support

- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support

- Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents

- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying

- Government advice about security and privacy settings, blocking unsuitable content, and parental controls

- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world

- Let’s Talk About It provides advice for parents and carers to keep children safe from online radicalisation

- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online

- Lucy Faithfull Foundation StopItNow resource can be used by parents and carers who are concerned about someone’s behaviour, including children who may be displaying concerning sexual behaviour (not just about online)

- National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online

- Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games

- Parentzone provides help for parents and carers on how to keep their children safe online

- Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations

- UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online

Relevant Legislation

Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2020
- Searching, screening and confiscation: advice for schools

Glossary of Terms

Blog – Short for Web Log, an online diary

DFE - Department for Education

Podcast – a downloadable sound-recording that can be played on computers and MP3 players

Social Networking – websites that allow people to have “pages” that allow them to share pictures, video and sound and information about themselves with online friends. Often, users do not have 100% control over content as friends can upload photos/videos/etc. to their pages at will. Popular networks are Facebook, Twitter, mySpace, Tumblr, but there are many others and, when used safely and correctly, offer a valuable networking tool between colleagues and friends.

Video Blogging – online videos that can be uploaded

Web 2 Technologies – a collection of online web services that are based around communicating/sharing information