CHURCHILL
SCHOOL

Online Safety Policy

What is Online Safety?

Online safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school’s Online Safety Policy will operate in conjunction with other policies including those for pupil Behaviour, Bullying, Curriculum, Combined Data Protection and Freedom of Information, and PSHE. Additionally, it should be read in conjunction with The Prevent Duty - Departmental Advice for schools and childcare providers and Keeping Children Safe in Education Statutory Guidance for Schools and Colleges.

- Online safety concerns safeguarding children and young people in the digital world.
- Online safety emphasises learning to understand and use new technologies in a positive way.
- Online safety is less about restriction and more about education about the risks as well as the benefits so we can feel confident online.
- Online safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

Good Habits

Online safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of Online Safety Policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of content filtering.
- National Education Network standards and specifications.

The school will appoint a named Online Safety Lead to ensure online safety is embedded across the school.

The Online Safety Lead is - Mrs Kirsty Richards, Deputy Headteacher

Why is Internet use Important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school’s management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use Benefit Education?

Benefits of using the Internet in education include:

- Access to learning wherever and whenever convenient
- Access to world-wide educational resources including museums and art galleries
- Educational and cultural exchanges between pupils world-wide
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice
- Collaboration across support services and professional associations
- Improved access to technical support including remote management of networks and automatic system updates
- Exchange of curriculum and administration data with associated Local Authorities and the Department of Education

How Can Internet Use Enhance Learning?

- The school's Internet access will be designed expressly for pupil use and include filtering appropriate to the age of pupils
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support 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

Roles and Responsibilities

Governors and Headteacher

It is the overall responsibility of the Headteacher with the Governors to ensure that there is an overview of online safety as part of the wider remit of safeguarding across the school with further responsibilities as follows:

- The Headteacher has a designated Online Safety Lead to implement agreed policies, procedures, staff training, curriculum requirements and take responsibility for ensuring online safety is addressed in order to establish a safe ICT learning environment. All staff and pupils are aware of who takes this role within the school

- The Headteacher is responsible for promoting Online Safety across the curriculum and has an awareness of how this is being developed and implemented.

- The Governors MUST ensure online safety is covered within an awareness of safeguarding and how it is being addressed within the school. It is the responsibility of Governors to ensure that all safeguarding guidance and practices are embedded.

- The Safeguarding Governor challenges the school about having appropriate strategies which define the roles and responsibilities for the management, implementation and safety for using ICT, including:

  - Firewalls
  - Anti-virus and anti-spyware software
  - Filters or using an accredited ISP (Internet Service Provider)
  - Awareness of wireless technology issues
  - A clear policy on using personal devices and that any misuse or incident has been dealt with appropriately according to policy.

School Online Safety Lead

It is the role of the designated Online Safety Lead to:

- Appreciate the importance of online safety within the school and recognise that all educational establishments have a general duty of care to ensure the safety of their pupils and staff.

- Establish and maintain a safe ICT learning environment within the school.

- Ensure that up-to-date information and training is available for all staff to teach online safety and for parents to feel informed and know where to go for advice.

- Ensure that filtering is set to the correct level for staff and pupils, in the initial set up of a network, stand-alone PC, staff/student laptops and the school learning platform.

- Ensure that all adults are aware of the filtering levels and why they are there to protect pupils.

- Report issues and update the Headteacher.

- Liaise with the relevant staff to ensure that policies and procedures are up-to-date to take account of any emerging issues and technologies.

- Update staff training according to new and emerging technologies so that the correct online safety information can be taught or adhered to.

- Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified.

- Refer to the appropriate policies to ensure the correct procedures are used with incidents of misuse.

The ICT Department

The ICT Department is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensuring there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-alone PCs and laptops and that this is reviewed and updated on a regular basis.

- Ensuring that staff can check for viruses on laptops, stand-alone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.

- Ensuring that unsolicited e-mails to a member of staff from other sources is minimised.

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

- Conducting a full security check and monitoring the school's ICT systems.

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

All staff and volunteers

All staff, agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use.
- Working with the Designated Safeguarding Lead to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour Policy

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.

Safeguarding Measures - Filtering

The school is responsible for setting its filtering systems. It is the responsibility of the Governing Body and the Headteacher to ensure that the filtering systems protect young people from inappropriate materials. The levels listed below are in relation to age appropriate categories:

- Staff - Basic adult policy. This allows for some customisation and the addition of sites if agreed by the IT Network Manager

• Students – Basic student policy. All sites are blocked except for accepted sites provided by staff, checked by the IT Manager and that conform to safe search protocols.

• Internet search engines are forced through ‘safe search’ as a matter of course, as are ‘You Tube’ and similar products.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access
- All staff must read and sign the ‘Acceptable ICT Use Agreement’ before using any school ICT resource

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the ICT department
- Churchill School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

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 personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Access in school to external personal e-mail accounts may be blocked
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- The forwarding of chain letters is not permitted

Social Networking

- The school will block/filter access to social networking sites and newsgroups unless a specific use is approved
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils will be advised not to place personal photos on any social network space
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others

Video Conferencing

- IP video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet

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
- Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden
- Currently there are no methods of SMS contact with parents and pupils

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will be appropriate for the context
- Pupils' full names will not be used anywhere on the Website, or any publications, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published.

Information System Security

- School ICT systems capacity and security will be reviewed regularly
- Virus protection will be installed and updated regularly
- Security strategies will be discussed with appropriate authorities.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.

The school cannot accept liability for the material accessed, or any consequences of Internet access.

Handling Online Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the Headteacher unless it concerns the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with safeguarding procedures
- Pupils and parents will be informed of the complaints procedure

How will infringements be handled?

Whenever a pupil or staff member infringes the Online Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

Sanctions will be set dependent on the nature of the offence and advice will be sought.

Educating pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use Meeting Time to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Educating parents about Online Safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website and the Churchill App. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

Preventing and addressing cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Behaviour Policy.)

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health education (PSHE) and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The Designated Safeguarding Lead will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the Department of Education's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Pupils using mobile devices in school

Pupils may bring mobile devices into school. However, with the exception of sixth form pupils, these must be handed into the office and are stored in a locked cupboard until they are collected at the end of the day.

Any use of mobile devices in school by pupils must be in line with the Acceptable Use Agreement.

Any breach of the Acceptable Use Agreement by a pupil may trigger disciplinary action in line with the school Behaviour Policy, which may result in the confiscation of their device.

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

Managing Social Networking and Other Web 2.0 Technologies

Social networking sites have emerged in recent years as a leading method of communication proving increasingly popular amongst both adults and young people alike. The service offers users both a public and private place through which they can engage with other online users. With responsible use, this technology can assist with the development of key social skills whilst also providing users with access to a range of easily accessible, free facilities. However, as with any technology that opens a gateway to online communication with young people, there are a number of risks associated which must be addressed. With this in mind, both staff and pupils are encouraged to think carefully about the information which they provide on such websites and the way in which it can be manipulated when published (examples of which include Facebook, Twitter and Snapchat). In response to this issue the following measures should be put in place:

- The school controls access to social networking sites through existing filtering systems.
- Pupils are advised against giving out personal details or information, which could identify them or their location (e.g. mobile phone number, home address, school name, groups or clubs attended, IM and email address or full names of friends).
- Pupils are discouraged from posting personal photos on social networking sites without considering how publicly accessible the information is and the potential for misuse. Advice is also given regarding background images in photos, which could reveal personal details (e.g. house number, street name, school uniform).
- Pupils are advised on social networking security and recommendations made for privacy settings to be activated to 'Friends only' for all applications to restrict unsolicited access. The importance of passwords and blocking of unwanted communications is also highlighted.

- The school is aware that social networking can be a vehicle for cyber bullying. Pupils are encouraged to report any incidents of bullying to the school, allowing for the procedures, as set out in the Behaviour Policy, to be followed.
- Social networking outside of work hours, on non-school equipment, is the personal choice of all staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking in conjunction with the training given in their Safeguarding training.
- Personal details such as private e-mail address, telephone number or home address are never shared with pupils. It is recommended that staff ensure that all possible privacy settings are activated to prevent pupils from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff should not engage in personal online contact with pupils outside of authorised systems (e.g. email account for homework purposes).
- Staff should ensure that full privacy settings are in place to prevent pupils from accessing photo albums or personal information.
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by pupils).
- There is well documented evidence to suggest that social networking can be a highly effective tool for communicating with pupils on a professional level. As such, professional communications using school e-mails and the VLE are permitted. Any abuse of this system should be reported to the relevant member of staff (line manager, any member of SLT or Headteacher).

Training

All new staff members will receive a copy of this policy and safeguarding training, as part of their induction.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through e-mails, e-bulletins and staff meetings).

The Designated Safeguarding Lead [and deputy] will undertake safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

How will staff and pupils be informed of these procedures?

- They will be fully explained and included within the school’s Online Safety and Acceptable Use Policies. All staff will be required to sign the school’s Acceptable Use Agreement.

- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop ‘safe behaviours’. Pupils will sign an age appropriate acceptable use form as part of the admission arrangements and an annual class agreement.
- The school’s Online Safety Policy will be made available to parents.
- Information on reporting abuse / bullying etc. will be made available by the school for pupils, staff and parents.

Review

This policy will be reviewed in line with the school’s policy review programme.

Author Kirsty Richards	**Date** Spring Term 2019	**Frequency of Review** Three Yearly
Adopted by the Governing Body Date: Signed	**Reviewed** Date: Signed	**Reviewed** Date: Signed