



BOLNEY CEP SCHOOL

Online Safety Policy

Online safety is not really about technology – it is about people and their actions. Technology provides new learning opportunities – online collaboration, anytime anywhere learning and communication. However there are negative aspects to technology, such as, the opportunity for students to access unsuitable material and the potential for students to be treated inappropriately.

Learning about online safety is a vital life skill. Empowering children at an early age with the knowledge to safeguard themselves and their personal information is something that needs to be nurtured throughout school to see them into adult life.

Bolney School believes in the whole school approach to ensure that all staff can recognise and are aware of online safety issues, that the senior leadership team make it a priority across all areas of the school, with a commitment to training, the development of policies, and a straightforward consistent approach when tackling an incident.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community
- The Headteacher/Senior Leaders are responsible for ensuring that the online safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant
- The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- The Headteacher/Senior Leaders should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff

Information System Security:

- School IT systems capacity and security will be reviewed regularly
- Virus protection will be installed and updated regularly by JSPC



Be the Best You Can,
Guided by God

Online Safety Policy
Reviewed June 2022
Review due Autumn 2024

The Computing (Online Safety) Lead:

- Has a leading role in establishing and reviewing the school online safety policy/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Provides training and advice for staff
- Liaises with school ICT technical staff (JSPC)
- Receives details of online safety incidents and creates a log of incidents to inform future online safety developments

Authorised Internet Access:

By explicitly authorising use of the school's Internet access pupils, staff, governors and parents are provided with information relating to online safety and agree to its use:

- All staff must read and sign the 'Acceptable IT Use Agreement' before using any school IT resource
- Parents will be informed that pupils will only access the Internet in the company of school adults and asked to sign and return a consent form for pupil access
- Only authorised equipment, software and Internet access can be used within the school, pupils are not to access the Internet using personal smart watches unless there is an appropriate medical reason, eg continuous glucose monitoring
- Children are taught how to use the equipment and Internet appropriately and safely

Published Content and the School Website

The school website is a valuable source of information for parents/carers and potential parents/carers.

- Contact details on the website will be the school address, e-mail and telephone number
- Staff and pupils' personal information will not be published
- The Headteacher or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate
- Pupils' full names will not be used in association with photographs
- Consent from parents will be obtained before photographs of pupils are published on the school website by an overarching consent form, children will be asked for their permission to use any photo or video at the time of using.
- Work will only be published with the permission of the pupil
- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy



Be the Best You Can,
Guided by God

Online Safety Policy
Reviewed June 2022
Review due Autumn 2024

Use of the Internet/devices in school:

E-mail

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of online safety:

- 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
- Whole class or group e-mail addresses should be used in school rather than individual addresses
- Access in school to external personal e-mail accounts is not allowed

Security and passwords:

Passwords should be changed regularly. The system will inform users when the password is to be changed. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff must always 'lock' the PC if they are going to leave it unattended.

Digital/Video Cameras/Photographs:

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff
- Publishing of images, video and sound will follow the policy set out in this document under 'Published Content'
- Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background
- The Headteacher or a nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner
- Staff should always use a school camera/iPad to capture images and should not use their personal devices
- Photos taken by the school are subject to the Data Protection Act
- Children should not use their own devices to take videos or photographs, ie smart watches



Be the Best You Can,
Guided by God

Online Safety Policy
Reviewed June 2022
Review due Autumn 2024

Educating children about online safety:

The Internet is an essential element for education, business and social interaction. It is a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience as part of the computing curriculum, all year groups have digital literacy units that focus on different elements of staying safe on line. These units include topics from how to use a search engine, digital footprints and cyber bullying (online bullying). Swiggle or Kiddle are search engines we regularly use.

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils to only have access to the internet when they are in the company of adults.

In Key Stage 1, pupils will be taught to:

- 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

Pupils in Key Stage 2 will be taught to:

- 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
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- By the end of primary school, pupils will know:
 - That people sometimes behave differently online, including by pretending to be someone they are not
 - That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
 - The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
 - How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
 - How information and data is shared and used online
 - How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The school Internet access will be designed expressly for pupil use including appropriate content filtering
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not



Be the Best You Can,
Guided by God

Online Safety Policy
Reviewed June 2022
Review due Autumn 2024

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Use of Social Media:

Social networking Internet sites provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Acceptable Use Policy.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites
- School staff use Twitter to quickly share and celebrate children's achievements, successes and school updates. There are two accounts, one is only for school families who need to be accepted to join, the other is open to the world and is used to celebrate school events, no images where children's faces can be recognised are used on this account. The



Be the Best You Can,
Guided by God

Online Safety Policy
Reviewed June 2022
Review due Autumn 2024

use of Twitter also enables the children to learn about a safe and responsible way of using social media.

- There is a school Facebook page with minimal content, this is monitored by Zoe Belton, SBM
- There is a Friends of Bolney Facebook page overseen by the PTA and is used as a communication tool to inform parents of any fundraising or special events.
- The Friends of Bolney have class Whats App groups for quick messaging, this is monitored by a parent from each class, it is only used for sharing relevant school information

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the Anti-Bullying policy)

Preventing and addressing cyber-bullying:

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. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Relationships and Health Education (RHE), 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.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy and the anti-bullying 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 DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.



Be the Best You Can,
Guided by God

Online Safety Policy
Reviewed June 2022
Review due Autumn 2024

Examining electronic devices (mobile phones, smart watches, activity trackers):

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, smart watches, activity trackers, 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 the material, or
- Retain it as evidence (of a possible criminal offence* or a breach of school discipline), and/or
- Report it to the police**

* If a staff member believes a device may contain a nude or semi-nude image or an image that it is a criminal offence to possess, they will not view the image but will report this to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#).

** Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure



Be the Best You Can,
Guided by God

Online Safety Policy
Reviewed June 2022
Review due Autumn 2024

Pupils use of personal devices in school, including mobile phones, activity trackers, smart watches:

- Pupils in Y5 and Y6 can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use, ie walking to and from home or the park without an adult. Mobile phones are handed into the school office on arrival and collected at the end of the day
- The sending of abusive or inappropriate text messages is forbidden

Staff use of mobile phones and devices (laptops/hard drives) in and out of school:

- Staff should always use the school phone to contact parents, where possible or use the 141 withheld number code if phoning from personal phone
- Staff, including students and visitors, are not permitted to access or use their mobile phones within the classroom. All staff, visitors and volunteers should ensure that their phones are turned off (if stored in the classroom) and stored safely away during the teaching day.
- A mobile phone can be used for medical monitoring following permission from the head teacher, eg continuous glucose monitoring
- Staff may use their mobile phones in the staffroom/one of the school offices
- School mobile phones and devices used for communication with parents and pupils must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff
- On trips staff mobiles are used for emergency only
- Ensuring the laptop hard drive, and any other portable hard drive, is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always install the latest updates (JSPC)

Educating Staff and Volunteers:

All staff, including contractors and 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 IT systems and the internet and ensuring that pupils follow the school's terms on acceptable use



Be the Best You Can,
Guided by God

Online Safety Policy
Reviewed June 2022
Review due Autumn 2024

- Working with the DSL 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 and anti-bullying policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

Educating parents/carers about online safety:

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 IT systems and internet
- Parents' and carers' attention will be drawn to the school Online Safety Policy in newsletters and on the school website, we also inform parents of Safer Internet Day and the resources available
- Parents and carers receive a termly online safety newsletter with up to date information regarding games/apps and latest safety advice with resources suggested for discussion at home

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

<http://www.saferinternet.org.uk/>

<https://www.betterinternetforkids.eu/>

<http://www.childnet.com/>

<http://www.thinkuknow.co.uk/>