ONLINE SAFETY POLICY

Reviewed by:	Impact Committee
Date reviewed:	December 2021
Next review:	December 2024 (every three years)
Member of staff responsible:	Natalie Hancock, Deputy Headteacher

1. Aims

Our school aims to:

● Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors

● Deliver an effective approach to online safety, which empowers us to protect and educate the

● whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')

● Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

● **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism

● **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

● **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

● **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools

- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

- Relationships and sex education

- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and responsibilities

3.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety incidents.

All governors will:

- Ensure that they have read and understand this policy

- Agree and adhere to the terms in 'Staff IT Acceptable Use Policy'

- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the Headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents

- Managing all online safety issues and incidents in line with the school child protection policy

- Ensuring that any online safety incidents are logged on Satchel One and/or CPOMS and dealt with appropriately in line with this policy

● Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

● Updating and delivering staff training on online safety

● Liaising with other agencies and/or external services if necessary

● Providing regular updates on online safety in school to the Headteacher and/or Governing Body

3.4 The ICT Team

The ICT Team is responsible for:

● Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

● 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 on a regular basis

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

● Ensuring 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.

3.5 All staff and volunteers

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

● Maintaining an understanding of this policy

● Implementing this policy consistently

● Agreeing and adhering to the Staff IT Acceptable Use Policy and ensuring that pupils follow the school's terms on acceptable use (Appendix 1)

● 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

● 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'

3.6 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 (appendix 1)

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

● What are the issues? – UK Safer Internet Centre

● Hot topics – Childnet International

● Parent resource sheet – Childnet International

● Healthy relationships – Disrespect Nobody

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected adhere to the Staff IT Acceptable Use Policy

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. Referenced also in the RSE (Relationship and Sex Education Policy)

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

● To understand how changes in technology affect safety, including new ways to protect their online privacy and identity

By the **end of Key Stage Four**, pupils will know:

● Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online

● About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online

● Not to provide material to others that they would not want shared further and not to share personal material which is sent to them

● What to do and where to get support and manage issues online

● The impact of viewing harmful content

● That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners

● That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail

● How information and data is generated, collected, shared and used online

● How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

● How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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.

5. 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. This policy will also be shared with parents.

Online safety will also be covered by our School's Police Liaison Officer

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

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

6. Cyber-bullying

6.1 Definition

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's Behaviour For Learning Policy.)

6.2 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. Tutors will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Personal, Social, Health and Citizenship (PSHCE) education, and other subjects where appropriate.

LT (Leadership Team and HOKS (Heads of Key Stages) will cover this topic in assemblies throughout the year

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information 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 for Learning 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 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.

All students at Chipping Norton School know that they can report any issues, concerns or worries through our confidential email address safe@chippingnortonschool.org

They will be supported and dealt with sensitively and in line with our Behaviour For Learning Policy and Child Protection Policy.

6.3 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*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

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

●   The DfE's latest guidance on screening, searching 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.

7. Acceptable use of the internet in school

All pupils and parents, are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendix 1). All staff, volunteers and governors will be expected to read and agree to the Staff IT Acceptable Use Policy

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them at the following times unless the teacher has granted permission:

●   Lessons

●   Tutor time

●   Break times

●   After school clubs /activities

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school Behaviour for Learning Policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

● Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters

● Ensuring their 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 – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in the Staff IT Acceptable Use Policy

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the IT Team (Turn It On)

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our Behaviour for Learning Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Code of Conduct and Disciplinary Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates via the Staff Bulletin. By way of this training, all staff will be made aware that Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse Children can abuse their peers online through:

● Abusive, harassing, and misogynistic messages

● Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

● Sharing of abusive images and pornography, to those who don't want to receive such content

●   Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

●   Training will also help staff:

●   develop better awareness to assist in spotting the signs and symptoms of online abuse

●   develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up

●   develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSLs will undertake child protection and 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.

12. Monitoring arrangements

The Pastoral Team will log and monitor behaviour and safeguarding issues related to online safety on Satchel One and/or CPOMS

This policy will be reviewed every 3 years by the Impact Committee of the Governing Body.

13. Links with other policies

This online safety policy is linked to our:

●   Child protection and safeguarding policy

●   Behaviour For Learning Policy

●   Staff Code of Conduct

●   Disciplinary Policy

●   Data protection policy and privacy notices

●   Complaints procedure

●   Staff IT Acceptable Use Policy

Appendix 1: Acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

● Always use the school's ICT systems and the internet responsibly and for educational purposes only

● Only use them when a teacher is present, or with a teacher's permission

● Keep my username and passwords safe and not share these with others

● Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer

● Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others

● Always log off or shut down a computer when I'm finished working on it

I will not:

● Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity

● Open any attachments in emails, or follow any links in emails, without first checking with a teacher

● Use any inappropriate language when communicating online, including in emails

● Log in to the school's network using someone else's details

● Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

● I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission

● I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):	Date:

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	Date: