School Spider

ONLINE SAFETY

A GUIDE FOR YOUR SCHOOL

CONTENTS

OFSTED GUIDELINES

From September 2020, Ofsted issued further guidelines regarding e-safety provisions in schools. Ofsted now lookout for how the schools protect and educate staff and pupils in its use of technology, along with what measures the school have in place to intervene and support should an issue arise.

EXPECTATIONS

- Teaching and non-teaching staff should be aware and able to recognise e-safety issues.
- Training given to all staff which must be continuous. One member of staff to receive accredited training.
- Clear reporting process for any issues that arise.
- Plain English policies and procedures. These must be integrated with other relevant policies.
- Progressive e-safety curriculum.
- Provisions in place by a recognised internet provider with age related filtering.
- Good risk assessment.
- Appropriate filters and monitoring systems.
- Ensure they teach their pupils about safeguarding, including online.

CURRICULUM

Teaching staff play a pivotal role in helping children understand the online world and how to stay safe. Ofsted want to see that teachers are implementing e-safety across the curriculum and how it is taught.

Curriculum Context

- Planned online safety programme.
- Taught across all age groups and progresses with age.
- Include what positive, healthy and respectful online relationships look like
- Effects of their online behaviour and recognising others
- Incorporate and make use of relevant initiatives such as Safe Internet Day.
- Accessible to pupils at different ages and abilities such as SEN or those who have English as an additional language.
- Pupils should be able to recall, explain and actively use online safety.
- E-safety should be in all appropriate lessons such as PSHE, sex and relationships and ICT.

KNOWLEDGE & BEHAVIOUR

It is important to focus on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. This teaching could be built into existing lessons across the curriculum, covered within specific online safety lessons and/or school wide approaches. Teaching must always be age and developmentally appropriate.

Underpinning knowledge and behaviours include:

- How to evaluation what they see online
- How to recognise techniques used for persuasion
- Online behaviour and recognising acceptable and unacceptable behaviour
- How to identify online risks
- How and when to seek support

YOU SHOULD INCLUDE

The harm and risks

Navigating and managing info

How to stay safe online

Wellbeing

POLICIES

All your school policies need to be freely and readily available in your school and via your website. Your policies need to be in plain English and specific to your school. They need to be known by pupils, staff and parents/guardians.

YOUR POLICY SHOULD INCLUDE:

Roles and responsibilities: Headteacher, governors, e-safety coordinator etc. How do they contribute to e-safety?

Define different technologies: Websites, emails, instant messaging, social media, mobile phones etc.

Link to other relevant policies: Link other relevant policies with e-safety; Acceptable use, child protection, anti-bullying etc.

Staff training: Details of training. Who has been trained and when this should be refreshed. Teaching and non-teaching staff should all have training. One member of staff should do accredited training.

Statements of pupils with SEN: Pupils with SEN have increased risk and so the policy should outline provisions in place to protect them.

Curriculum: What are children taught about e-safety in lessons? How it is embedded across the curriculum?

Misuse or breach of policy: How the school will respond to misuse of technology or a breach of the policy by staff or pupils.

How incidents area reported: How they are reported and how they are logged. These need to be well defined and clear. There needs to be clear procedures in place for responding to different online risks (cyber bullying, radicalisation, sexting, online grooming). Online report mechanism for pupils or parents to report an incident (CEOP).

Parent involvement: How parents are consulted about the policy and how the school involve them in promoting e-safety. Include how images and films are managed.

Management of email: Password security for your emails. What do you do if you receive or send an offensive email?

Statements on passwords and security: How are passwords kept and what happens if a password is shared?

Statements on the use of mobile technologies: When and how mobiles are used in school and sanctions for misuse

Use of webcams: When and how they will be used, measures in place to keep children safe and sanctions for misuse.

Video conferencing: When and how video conferencing is used in school and what measures are in place to safeguard children.

Monitoring and evaluation: How the school will monitor the effectiveness of the policy and e-safety practices and update when necessary.

SUPPORTING PARENTS

There are lots of worries and concerns about what children can face online, so involving parents and carers in learning about online safety is extremely important. This should be a key part of a whole school approach to e-safety.

Parental engagement

- Organise sessions where pupils can teach parents or carers what they know about e-safety.
- Regularly share resources with parents through newsletters, your website and flyers/posters throughout the school.
- Show parents the learning resources you use in the classroom.
- Circulate your e-safety policy to parents.

Useful Links:

https://www.saferinternet.org.uk/advice-centre/parents-and-carers

https://www.thinkuknow.co.uk/parents/

http://www.childnet.com/parents-and-carers

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

THINK

Safe

Keep safe by not giving out personal information when you're talking or posting online. This includes your email address, phone number and password.

Meet

Meeting someone you have only spoken to online can be dangerous. Only do so with your parents' permission and when they can be present. Remember, online

Accepting

Accepting emails, instant messages or opening files, images or texts from people you don't know, or trust can lead to problems – they may contain viruses or nasty messages.

Reliable

Someone online may lie about who they are and information on the internet may not always be true. Always check information you read and if you're chatting online it's best to speak to friends and family you know.

Tell

Tell a parent, carer or trusted adult if someone or something makes you feel uncomfortable or worried. You should also tell someone if you know someone is being bullied online.

SUPPORTING CHILDREN

Teaching staff play a pivotal role in helping children understand the online world and how to stay safe. Ofsted want to see that teachers are implementing e-safety across the curriculum and how it is taught.

Curriculum

- Planned online safety programme.
- Taught across all age groups and progresses with age.
- Continued online safety lessons.
- Incorporate and make use of relevant initiatives such as Safe Internet Day.
- Use of appropriate and up to date sources.
- Accessible to pupils at different ages and abilities such as SEN or those who have English as an additional language.
- Pupils should be able to recall, explain and actively use online safety.
- E-safety should be in all appropriate lessons such as PSHE, sex and relationships and ICT.

You will need to have a report mechanism for pupils to report an incident (CEOP is commonly used) and procedures in place for how you will respond to different reports.

STAFF TRAINING

Staff training needs to be given to all teaching and non-teaching staff to comply with Ofsted's requirements. Ofsted will look that expertise on online safety have been developed across all staff. Your training will need to be continuous and the content updated to reflect current research and advances in technology.

EXPECTATIONS

- Keep audit of all training that has been given.
- Training needs to be given at least annually.
- Online training needs to be by a recognised individual or a group with online safety responsibility.
- One member of staff should do accredited training to become an e-safety officer.
- Keep up with ever changing online technology

WAYS TO IMPLEMENT

- E-safety lessons to review and update policies.
- Display your e-safety rules around the school.
- Ensure staff are aware of the measures you have in place if they are found misusing technology.
- Report if you see other staff members misusing technology.

DATA PROTECTION

Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools in England to ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system. However, schools will need to be careful that over blocking does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

Schools need to have appropriate filters and monitoring systems in place, so children cannot access harmful content via the school's IT and any concerns can be spotted quickly

> *Treat your password like a toothbrush, don't let anyone use it and change it every six months*
>
> Clifford Stoll

MONITORING

Although no amount monitoring can guarantee to be 100% effective, schools should be satisfied that their monitoring strategy or system at least covers the following content:

Illegal Content that is illegal such as child abuse and terrorism.

Bullying Involving the repeated use of force, threat to abuse, intimidate or aggressively dominate others.

Child sexual exploitation Content where children could be encouraged to be involved in sexual relationships.

Discrimination Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity.

Drugs Displays or promotes the illegal use of drugs or substances.

Extremism Promotes terrorism and terrorist ideologies, violence or intolerance.

Pornography Displays sexual acts or explicit images.

Self harm Promotes or displays deliberate self harm.

Violence Displays or promotes the use of physical force intended to hurt others.

Suicide Suggest the user is considering suicide.

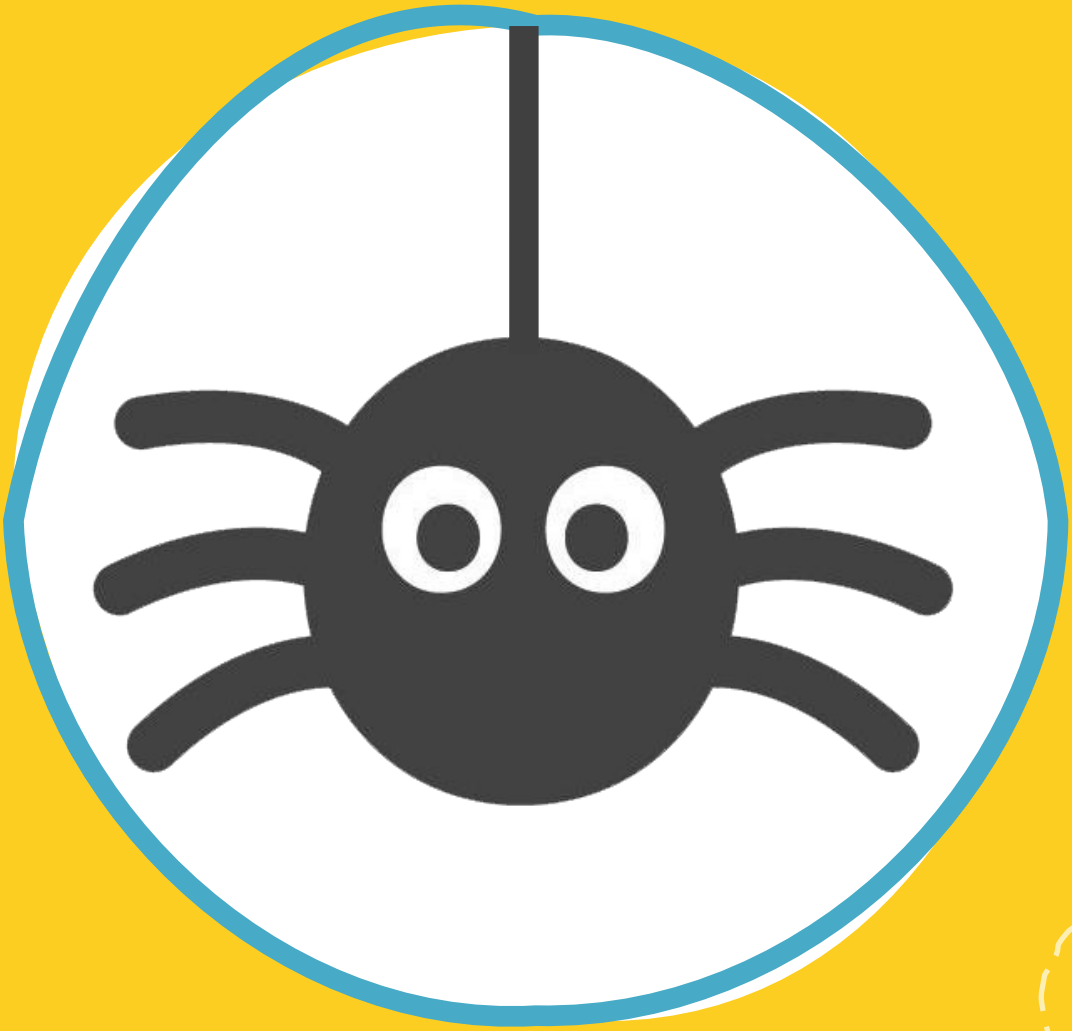
RESOURCES

Here is a list of links you can obtain other support and guidance online:

Government Guidance:

- Relationship Education, Relationships and Sex Education and Health Education Statutory Guidance
- Keeping Children Safe in Education - Statutory guidance for schools and colleges on safeguarding children and safer recruitment.
- CEOP Thinkuknow Programme: Online safety education programme from the National Crime Agency's CEOP Command which aims to safeguard children from sexual abuse and exploitation. Education resources and online advice for children aged 4 – 18
- National Centre for Computing Education (NCCE)
- UK Council for Internet Safety - The UK Council for Internet Safety expands the scope of the UK Council for Child Internet Safety to achieve a safer online experience for all users, particularly groups who suffer disproportionate harms.
- The Anti-Bullying Alliance
- Internet Matters – a not-for-profit organisation set up to empower parents and carers to keep children safe in the digital world,
- UK Safer Internet Centre

School Spider



Bring your school to life online!