# Kirk Smeaton C of E Primary School E Safety policy

To be reviewed March 22

## Introduction

This policy is written in conjunction with North Yorkshire E-safety guidance, safeguarding audit, curriculum policies, data protection policy, anti-bullying policy and safeguarding children policies and procedures. The Headteacher is the e-safety co-ordinator.

## Rationale

The internet and other digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning.

## Aims

Our aims are to ensure that all pupils, including those with special educational needs:

- will use the internet and other digital technologies to support, extend and enhance their learning;
- will develop an understanding of the uses, importance and limitations of the internet;
- digital technologies in the modern world including the need to avoid undesirable material;
- will develop a positive attitude to the internet and develop their ICT capability through both;
- ensure all users can access the internet and devices safely;
- independent and collaborative working;
- will use existing, as well as up and coming, technologies safely.

## Internet use will support, extend and enhance learning

- Pupils will be given clear objectives for internet use.
- Web content will be subject to age-appropriate filters in school.
- Internet safety will be given to parents to support them with home internet security.
- Internet use will be embedded in the curriculum.

## Pupils will develop an understanding of the uses, importance and limitations of the internet

- Pupils will be taught how to effectively use the internet for research purposes.
- Pupils will be taught to evaluate information on the internet.
- Pupils will be taught how to report inappropriate web content.
- Pupils will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working.
- Pupils will use the internet to enhance their learning experience.
- Pupils have opportunities to engage in independent and collaborative learning using the internet andother digital technologies.

## Data Protection

- There is a separate Data Protection policy.

## E-mail

- Pupils and staff will only use approved e-mail accounts when using the school network.
- Pupils will tell a member of staff and parents if they receive inappropriate e-mail communications, they will be supported in reporting these to https://www.ceop.police.uk/Safety-Centre/

## Internet Access and Learning Platform

- Staff will read and sign the NYCC Acceptable Use Policy – ICT and e-Technology before using any school ICT resource.
- Pupils will be taught to use the internet responsibly and to report any inappropriate content to a responsible adult. These are taught from the guidance published by the government in 2019 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf

## Mobile Phones and other handheld technology

Pupils are only permitted to have mobile phones or other personal handheld technology in school with the permission of the Headteacher. When pupils are using mobile technology (their own or that provided by the school) they will be required to follow the school's Acceptable Use Policy (AUP). Such items can be confiscated by school staff if they have reason to think that they are being used to compromise the wellbeing and safety of others (Education and Inspections Act 2006, Sections 90, 91 and 94).

School Website and Published Content

- There is a separate website policy.
- All staff who edit website content must read and sign this policy.

**Systems Security**

- ICT systems security will be regularly reviewed with support from Schools ICT.

**Web Filtering**

- The school will work with Schools ICT to ensure that appropriate filtering is in place.
- Pupils will report any inappropriate content accessed to an appropriate member of staff.

**School internet safety rules and procedures**

- E-safety rules are within the schools SHINE rules and are displayed around school.
- All children are given rules on how to behave on live lessons
- Pupils will be informed that internet and Learning Platform use will be monitored.
- e-Safety will be included in the curriculum and regularly revisited in accordance with the guidance from the government. Staff will use a PPT slides below (appendix A)
- Staff will be monitoring internet and Learning Platform.
- Communication of the e-safety policy to parents/carers
- The acceptable use policies will be available in the school prospectus and on the school website.
- The school website and dojo/tapestry will include a list of e-safety resources and information for parents to access.
- The school will communicate and publicise e-safety issues to parents through the school newsletter and website.

**Rules for live lessons**

1. All parties to be respectful.
2. All parties to mute their screens, unless they have been invited to speak by the host.
3. All parties can display their screen or disable the camera if they wish.
4. If the camera is displays, we ask for all parties to sit still and quiet during the session.
5. All parties are asked to wait a waiting room until they are asked to join the meeting. If they have not provided their first name and the first letter of the surname, they will be asked to change their name and they can be added to the meeting.
6. All meetings have a password and are recorded.
7. If children are accessing the live session from school, the camera will be disabled or directed at the teacher.
8. If someone wants to talk, they raise their hand.
9. Please be respectful with the chat facility and the content being shared.
10. Do not share the meeting ID or password with others and do not print screen or film the content being shared.

**E-safety Complaints**

- Instances of pupil internet or Learning Platform misuse should be reported to a member of staff.
- Staff will be trained so they are able to deal with e-Safety incidents. They must log incidents reported to them and if necessary refer the matter to a senior member of staff.
- Instances of staff internet or Learning Platform misuse should be reported to, and will be dealt with by, the Headteacher.
- Pupils and parents will be informed of the consequences of internet and/or Learning Platform misuse.

**Whole-School Responsibilities for Internet Safety**

**Headteacher**

- Responsible for e-safety issues within the school but may delegate the day-to-day responsibility to a member of staff.
- Ensure that developments at Local Authority level are communicated to the e-safety co-ordinator.
- Ensure that the Governing Body is informed of e-safety issues and policies.
- Ensure that appropriate funding is allocated to support e-safety activities throughout the school.
- Establish and maintain a school-wide e-safety programme.
- Form a school e-safety team to review and advise on e-safety policies.
- Work with the e-safety team to develop, and review, e-safety policies and procedures.
- Respond to e-safety policy breaches in an appropriate and consistent manner in line with protocols set out in policies, and maintain an incident log.
- Form a school e-safety management team to review the effectiveness and impact of the policy.
- Establish and maintain a staff professional development programme relating to e-Safety.
- Develop a parental awareness programme.
- Develop an understanding of relevant legislation and take responsibility for their professional development in this area.

**Governing Body**

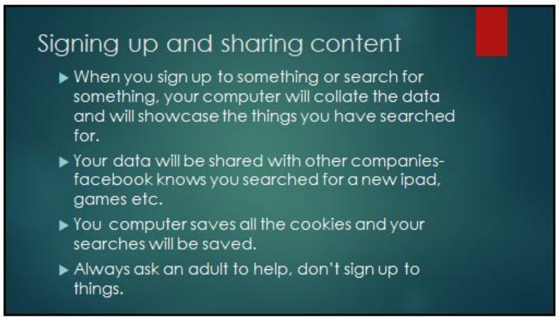
- Appoint an e-Safety Governor who will ensure that e-safety is included as part of the regular review of child protection and health and safety policies.
- Support the Headteacher and/or designated e-safety co-ordinator in establishing and implementing policies, systems and procedures for ensuring a safe ICT learning environment.

- Ensure that appropriate funding is authorised for e-safety solutions, training and other activities as recommended by the Headteacher and/or designated e-safety co-ordinator (as part of the wider remit of the Governing Body with regards to school budgets).
- Promote e-safety to parents and provide updates on e-safety policies within the statutory ‘security’ section of the annual report.

Appendix A

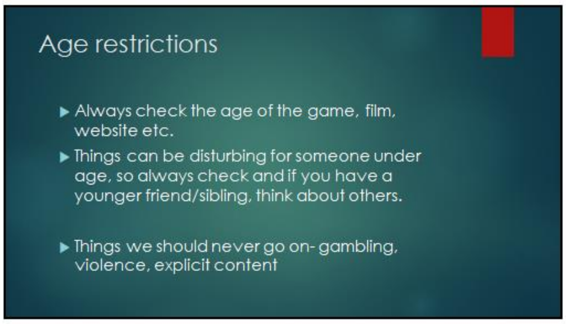
### Keeping safe online

OCT 20



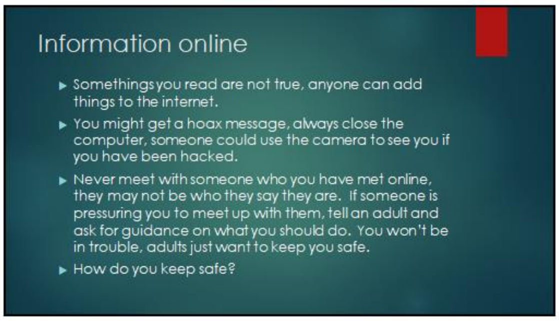
### Signing up and sharing content

- When you sign up to something or search for something, your computer will collate the data and will showcase the things you have searched for.
- Your data will be shared with other companies- facebook knows you searched for a new ipad, games etc.
- You computer saves all the cookies and your searches will be saved.
- Always ask an adult to help, don't sign up to things.



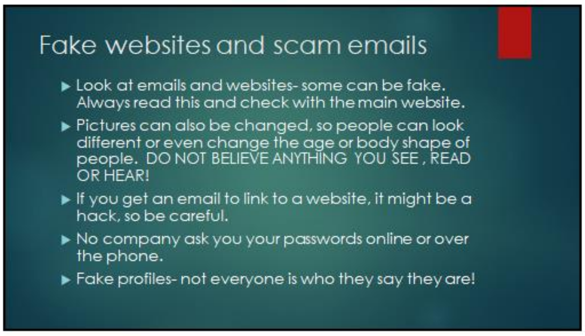
### Age restrictions

- Always check the age of the game, film, website etc.
- Things can be disturbing for someone under age, so always check and if you have a younger friend/sibling, think about others.
- Things we should never go on- gambling, violence, explicit content



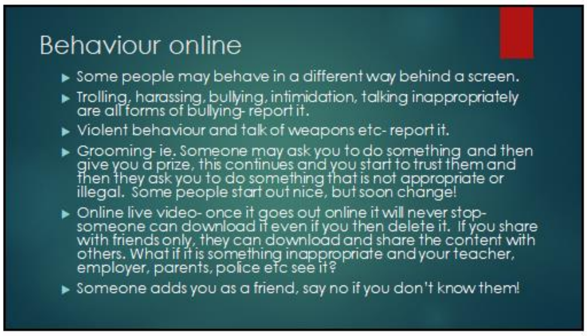
### Information online

- Somethings you read are not true, anyone can add things to the internet.
- You might get a hoax message, always close the computer, someone could use the camera to see you if you have been hacked.
- Never meet with someone who you have met online, they may not be who they say they are. If someone is pressuring you to meet up with them, tell an adult and ask for guidance on what you should do. You won't be in trouble, adults just want to keep you safe.
- How do you keep safe?



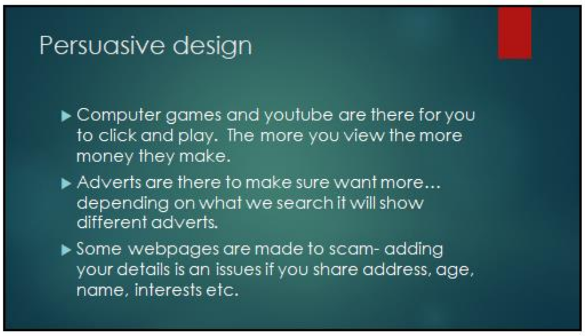
### Fake websites and scam emails

- Look at emails and websites- some can be fake. Always read this and check with the main website.
- Pictures can also be changed, so people can look different or even change the age or body shape of people. DO NOT BELIEVE ANYTHING YOU SEE , READ OR HEAR!
- If you get an email to link to a website, it might be a hack, so be careful.
- No company ask you your passwords online or over the phone.
- Fake profiles- not everyone is who they say they are!



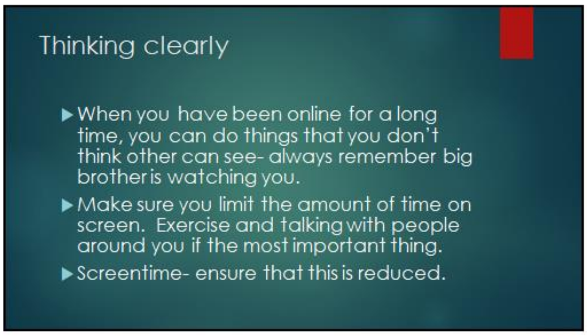
### Behaviour online

- Some people may behave in a different way behind a screen.
- Trolling, harassing, bullying, intimidation, talking inappropriately are all forms of bullying- report it.
- Violent behaviour and talk of weapons etc- report it.
- Grooming- ie. Someone may ask you to do something and then give you a prize, this continues and you start to trust them and then they ask you to do something that is not appropriate or illegal. Some people start out nice, but soon change!
- Online live video- once it goes out online it will never stop- someone can download it even if you then delete it. If you share with friends only, they can download and share the content with others. What if it is something inappropriate and your teacher, employer, parents, police etc see it?
- Someone adds you as a friend, say no if you don't know them!



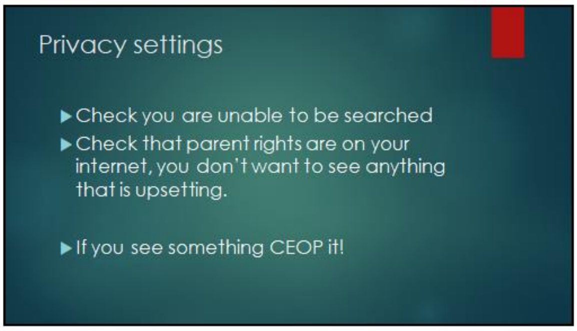
### Persuasive design

- Computer games and youtube are there for you to click and play. The more you view the more money they make.
- Adverts are there to make sure want more… depending on what we search it will show different adverts.
- Some webpages are made to scam- adding your details is an issues if you share address, age, name, interests etc.



### Thinking clearly

- When you have been online for a long time, you can do things that you don't think other can see- always remember big brother is watching you.
- Make sure you limit the amount of time on screen. Exercise and talking with people around you if the most important thing.
- Screentime- ensure that this is reduced.



### Privacy settings

- Check you are unable to be searched
- Check that parent rights are on your internet, you don't want to see anything that is upsetting.
- If you see something CEOP it!