CHRISTOPHER PICKERING PRIMARY SCHOOL

Online Safety Policy

Be the Best you can Be!

Head teacher: Mrs J Marson

Computing Leaders: Miss A Jeffrey, Mr J Sutton

Date: Autumn 2021

Review Date: Autumn 2022

Introduction

At Christopher Pickering Primary school, we understand the importance of teaching our children how to use the internet safely and responsibly. We know that children have the right to enjoy childhood online, to access safe online spaces, and to benefit from all the opportunities that a connected world can bring to them, appropriate to their age and stage. As they grow older, it is crucial that they learn to balance the benefits offered by technology with a critical awareness of their own and other's online behaviour and develop effective strategies for staying safe and making a positive contribution online.

The internet is essential in 21st century life for education, business and social interaction. As children move up through the school, their access to various types of technology increases and it stands to reason that their exploration and curiosity increases too. The positives of the digital world overwhelmingly outweigh the negatives but children, schools and parents all need to be aware of various online risks.

The policy covers the following key areas:

1. Potential risks of technical aspects
2. The School Network (maintenance and usage)
3. Pupil education on Internet Safety
4. Roles and responsibilities
5. Mobile Technologies
6. Digital and video imagery
7. Communications
8. Incidents / Breach of the policy
9. Social media
10. Ownership and Review

Potential risks

Potential risks of technical aspects that could leave pupils vulnerable if not understood include:

- Inappropriate content for age of the child
- How content is used and shared, including illegal content
- Disinformation, misinformation and hoaxes
- Fake website and scam emails
- Fraud (online)
- Password phishing
- Loss/misuse of personal data
- Persuasive design to keep children using devices/apps/games for longer

Potential risks of online activity that could adversely affect a pupil's personal safety or the personal safety of others online include:

- Abuse (online)
- Inappropriate challenges, including 'chain letter' style challenges
- Content which incites violence
- Fake profiles
- Grooming
- Live Streaming
- Pornography
- Unsafe communication

Potential risks of online activity that could adversely affect a pupil's well-being include:

- Impact on body confidence
- Physical, mental health and relationships
- Suicide, self-harm and eating disorders

How internet use at school is filtered and monitored

Christopher Pickering Primary School's Internet is provided by the East Riding Local Authority, whose filtering and reporting software helps us keep our students safe online and ensures our school is protected, meeting all of our safeguarding requirements. As well as being able to instantly request a block to sites, our internet is filtered using Smooth Wall, which is maintained by the East Riding Local Authority who ensure our school is safe from undesirable websites and images. Furthermore, their powerful and easy to use reporting portal notifies key staff of any potential risks in real time. This allows us as a school to react quickly and protect students or staff researching topics such as radicalisation, bullying, substance abuse or suicide. If any concerns are flagged, these are relayed back to the key stage of concern and intervention is put in place. Finally, during all computing lessons, staff visually monitor children's activity online.

How we teach children to stay safe online

In Key Stage 1 and Key Stage 2

Alongside the online safety content that is taught within our computing curriculum through Purple Mash and through the content covered through our PSHE curriculum with Jigsaw, we also follow the recommendations of the Education for a Connected World framework and use lessons from Project Evolve. This describes the knowledge, understanding and skills that children and young people should have the opportunity to develop at different ages and stages. It highlights what a child should know in terms of current online technology, its influence on behaviour and development, how to get support, and what skills they need to be able to navigate it safely. Children and young people's online activity and behaviour can be different both within and across an age range. This framework is intended to be used flexibly in order to support learning that is relevant to children and young peoples' online behaviour and experiences and matched to their readiness for new learning.

Furthermore, as a school we have a dedicated team of digital leaders, who play a powerful role in educating their peers – by providing relatable and up to date advice – and shaping our school's ethos by acting as role models. The ChildNet Digital Leaders Programme offers our children access to an exciting online community, where they access training and support from ChildNet's expert team and record achievements and progress. They also have the opportunity to collaborate and share inspiration with young Digital Leaders across the UK.

See our Christopher Pickering Online Safety Overview for the sequence and progression of Online Safety lessons taught in each year group.

Foundation Stage

At Christopher Pickering Primary School, we recognise that children can be exposed to age inappropriate games online, from a young age. Therefore, Staff in the Early Years Foundation Stage are vigilant when monitoring role play during continuous provision. If observations are made of games that are age inappropriate, feedback will be delivered to the parents. Furthermore, assemblies will be held with the year group to discuss PEG ratings on games and why these are needed.

Roles and responsibilities

The following section outlines the roles and responsibilities for Online Safety of individuals and groups within the school:

Governing Body:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

• Regular meetings with the Computing Co-ordinator

• Regular monitoring of Online Safety incident logs

• Reporting to relevant Governors' meetings

Head teacher and SLT:

• The Head Teacher/Safeguarding Lead is responsible for ensuring the safety (including Online Safety) of members of the school community, will be a joint responsibility of the Computing Co-ordinator, the Safeguarding Lead and Head Teacher.

• The Head Teacher/Safeguarding Lead is responsible for ensuring that the Computing 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 Head Teacher/Safeguarding Lead 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 Head Teacher and another member of the Senior Leadership Team 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.

Computing Leads will:

• Take day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies

• Ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place

• Provide training and advice for staff

• Liaise with school ICT technical staff

• Be aware of any Online Safety concerns that have been reported to the Safeguarding Lead, Deputy Safeguarding lead, Head teacher and Deputy Head and kept on record. Incidents will inform future Online Safety developments

• Meet regularly with the Online Safety Governor to discuss current issues, review incident logs and filtering

The ICT Technician and Computing Lead are both responsible for ensuring:

• That the school's ICT infrastructure is secure and is not open to misuse or malicious attack

• That the school meets the Online Safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance

• That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed

• That they keep up to date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant Teaching and Support Staff:

Teaching and support staff are responsible for ensuring that:

• They have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices.

• They have read, understood and signed the school Staff Acceptable Use Policy

• They report any suspected misuse or problem to the Computing Co-ordinator and the Deputy Head Teacher/Safeguarding Lead for investigation via CPOMs.

• Digital communications with pupils should be on a professional level

• Online Safety issues are embedded in all aspects of the curriculum and other school activities

• Pupils understand and follow the school Online Safety and acceptable use policy

• Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

• They monitor ICT activity in lessons, extra-curricular and extended school activities

• They are aware of Online Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices

• In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Safeguarding Lead:

The Safeguarding Lead should be trained in Online Safety issues and be aware of the potential for serious child protection issues to arise from:

• Sharing of personal data

• Access to illegal/inappropriate materials

• Inappropriate on-line contact with adults/strangers

• Potential or actual incidents of grooming

• Cyber-bullying

Pupils:

• Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which parents will be expected to sign before being given access to school systems.

• Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

• Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

• Should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school.

Digital Leaders

As a Digital Leader, children have the opportunity to:

• Deliver education sessions for young people in their school or community.

• Raise awareness online and offline about internet safety, for example a blog or making a poster

• Carry out a survey in order to find out more about young people's use of technology.

• Be an expert in their school by giving advice and support about a range of issues.

•Influence how their school and organisation helps ensure young people are using technology kindly, respectfully, creatively and responsibly.

•Run a campaign to address a key issue and change things for the better.

• Create an educational resource about internet safety.

Parents and Carers:

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and/or mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, and website. Parents and carers will be responsible for:

• Endorsing (by signature) the Responsible Use of the Internet Policy

Mobile Technologies

Legitimate recordings and photographs should be captured using school equipment such as cameras and IPads.

Staff should have their phones on silent or switched off and out of sight (e.g. in a drawer, handbag or pocket) during class time

Mobile phones should not be used in a space where children are present (e.g. classroom, playground)

Use of phones (including. receiving/sending texts and emails) should be limited to non-contact time when no children are present e.g. in office areas, staff room, empty classrooms

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students/pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press

- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school/academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *students/pupils* in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school/academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school/academy equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school/academy into disrepute.
- Students/pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Students'/Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Communication Technologies

When using communication technologies, the school considers the following as good practice:

- The official school email service is regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students/pupils should therefore use only the school/academy email service to communicate with others when in school, or on school/academy systems (e.g. by remote access).
- Users must immediately report, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- If a student/pupil brings a Mobile Phone into school, this must be switched off and handed in to the school office and collected at the end of the school day.
- Any digital communication between staff and students/pupils or parents/carers (email, social media, chat, blogs) must be professional in tone and content. These communications may only take place on official (monitored) school/academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- In KS2 Students/pupils will be provided with individual school/academy email addresses for educational use.
- Students/pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school/academy website and only official email addresses should be used to identify members of staff.

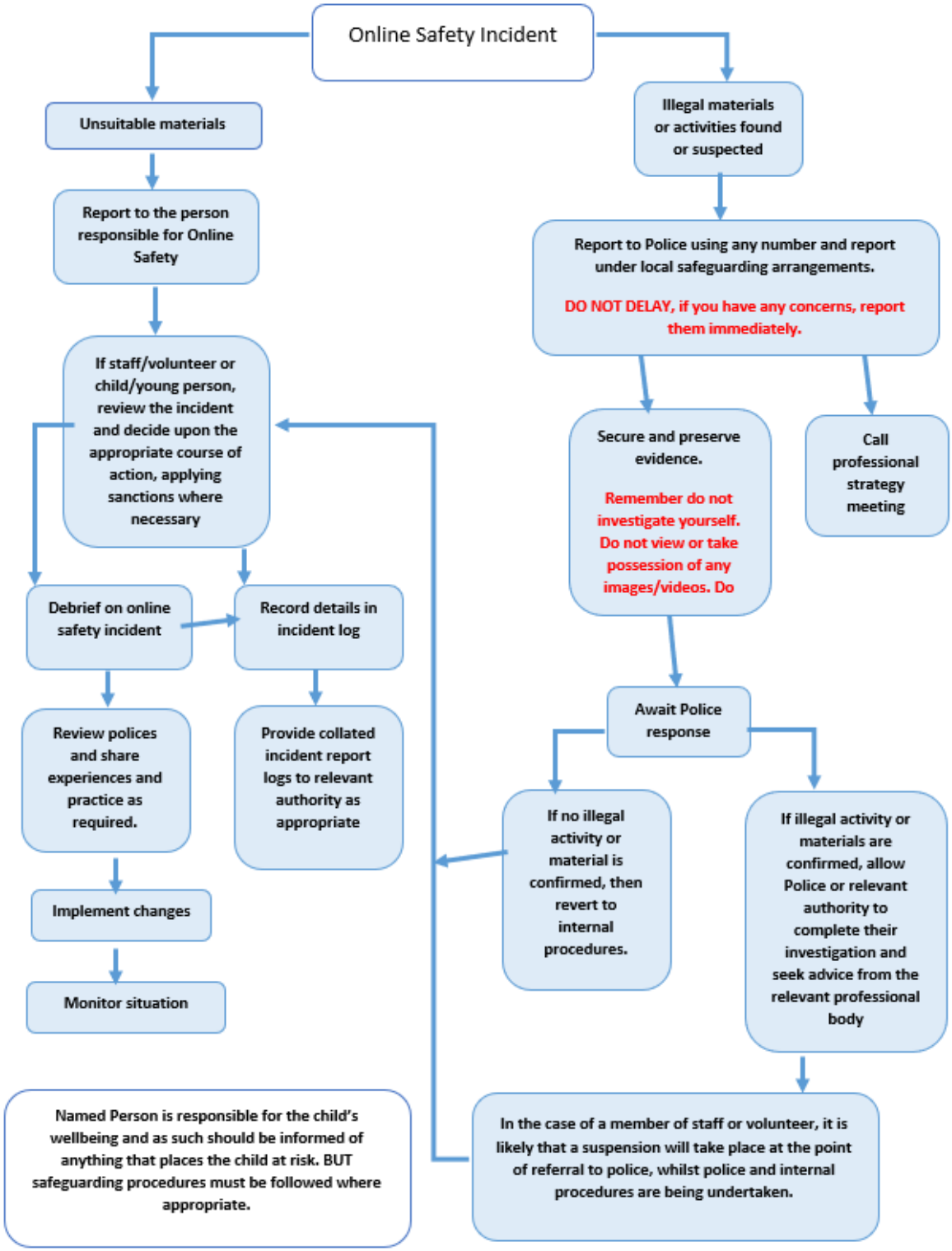
Incidents / Breach of the policy

- All incidents are dealt in accordance with the online safety incident flow chart (below) and must be reported to the Head Teacher. Parents are informed in the case of an online safety incident relating to their child.
- In the case of a serious incident, it may be reported to CEOP, social services or to the police.
- If the safety incident is a safe guarding incident, a cause for concern form will be completed.

- Unlawful or unsafe behaviour online and breaches of this policy are unacceptable. Where appropriate, disciplinary action may be taken and the Local Authority and or police services involved.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Social Media

The school/trust recognises and embraces the numerous benefits and opportunities that social media offers. While employees are encouraged to engage, collaborate and innovate through social media, they should also be aware that there are some associated risks, especially around issues of safeguarding, bullying and personal reputation.

Roles, responsibilities and procedure

Employees should:

- be aware of their online reputation and recognise that their online activity can be seen by others including parents, pupils and colleagues on social media;
- ensure that any use of social media is carried out in line with this policy and other relevant policies, i.e. those of the employer;
- be aware that any excessive use of social media in school/college may result in disciplinary action;
- be responsible for their words and actions in an online environment. They are therefore advised to consider whether any comment, photograph or video that they are about to post on a social networking site is something that they want pupils, colleagues, other employees of the trust, or even future employers, to read. If in doubt, don't post it!

Managers are responsible for:

- addressing any concerns and/or questions employees may have on the use of social media;
- operating within the boundaries of this policy and ensuring that all staff understand the standards of behaviour expected of them.

Acceptable use

Employees should be aware that content uploaded to social media is not private. Even if you restrict it to 'friends', there is still capacity for it to be re-posted or distributed beyond the intended recipients. Therefore, employees using social media should conduct themselves with professionalism and respect.

Employees should not upload any content on to social media sites that:

- is confidential to the school/trust or its staff
- amounts to bullying
- amounts to unlawful discrimination, harassment or victimisation
- brings the school/trust into disrepute
- contains lewd, sexually explicit, threatening or similarly inappropriate or offensive comments, images or video clips
- undermines the reputation of the school and/or individuals
- is defamatory or knowingly false
- breaches copyright
- is in any other way unlawful.

Employees should be aware of both professional and social boundaries and should not therefore accept or invite 'friend' requests from pupils or ex-pupils under the age of 18, or from parents on their personal social media accounts such as Facebook. All communication with parents via social media should be through the school/trust's social media accounts. Employees should note that the use of social media accounts during lesson time is not permitted.

Ownership of Policy and Review

This policy has been written by the following working group:

• Computing Coordinator – Miss A Jeffrey

• Curriculum Lead – Mrs Yardley

• Designated Safeguarding Lead/ Deputy Head teacher – Mrs L Leeman

•The Head teacher – Mrs Marson

The policy will be reviewed in Autumn 2022