General Policy Document

Document Name: Online Safety Policy

First Written Date: n/a

[Review Date: November 2020

Reviewed By: Governors

Ratified By Full Governors Date: November 2020

Next Review Date: October 2022

Document No: GP014

Online Safety Policy

General Policy Document

Document Name: Online Safety Policy
Review Date: November 2020
Reviewed By: Governors
Ratified By Full Governors Date: November 2020
Next Review Date: October 2022

Bramhope Primary School Online Safety Policy

This online safety policy documents how we work to ensure children, staff and other members of the school community with online access are safe when using the computer network at Bramhope Primary School. It sets out clear expectations of behaviour when online and defines clear structures and processes to deal with any online safety incidents. This policy should be read in conjunction with the staff and pupil acceptable use policies (AUP) and the other relevant school policies.

The policy covers the following key areas:

1. The School Network (maintenance and usage)
2. Mobile devices
3. Pupil / Parent / Staff education
4. Communications
5. Social media
6. Digital imagery
7. Remote Learning
8. Incidents / Breach of the policy
9. Roles and responsibilities
10. Ownership and Review

The school is fully committed to compliance with the General Data Protection Regulations. The GDPR requirements are covered in a separate policy.

1. The School Network – Maintenance

- The school meets recommended technical safety requirements.
- There are regular reviews and audits of the safety and security of the school technical systems.
- Servers, wireless systems and cabling are securely located and physical access restricted.
- The "administrator" passwords for the school system are kept only with the designated IT technician and the Head Teacher in a secure place.
- Software licence logs are accurate and up to date.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- All members of staff and pupils understand that any damage must immediately be reported to the Head Teacher.
- Any remote access provided must be authorised and secure.

The School Network – Usage

- All users have clearly defined access rights to school devices.
- All users must sign the relevant AUP before gaining access to the school IT systems.
- An agreed policy is in place for the provision of temporary access of "guests" with a dedicated supply teacher log on.
- Internet access is filtered for all users to ensure they are safe. There is a clear process in place to deal with requests for filtering changes.
- The school digital technology and communication is monitored with Light speed check carried out by the Head Teacher to protect against inappropriate content.
- Regular checks are carried out by the deputy designated safeguarding lead to check that the filtering system is effective.
- Any online breaches are reported to the Head Teacher and in accordance with the procedures set out in Appendix 1 – Dealing with online safety incidents.
- Staff and pupils understand that school devices are not to be used for personal or recreational use. Personal emails are not to be accessed on the school systems.
- Staff and all KS2 pupils have passwords to protect their work and the school computer system. It is their duty to keep these secure and to update them regularly.
- Use of the internet by pupils is adequately supervised at all times.
- All members of staff and pupils understand that they must immediately report any illegal, inappropriate or harmful material or incident to the Head Teacher.

2. Mobile Devices

- Staff and visitors are only permitted to use mobile devices (laptops/tablets/mobile phones / USB devices) in school at break times. All personal devices are stored in the class stockroom or staff room and cannot be accessed at any point in front of children.
- If pupils need to bring a phone to school, a declaration form must be filled in by the parent / carer and the phone signed into/out of the office at the beginning and end of the school day. Electronic devices which have internet access, are able to take images / audio / video recordings or send and receive messages are not permitted in school.
- Supply staff and visitors are reminded that mobile devices are not to be used in school in the presence of children.

3. Pupil / Parent / Staff Education

- Pupils and staff are aware of who is responsible for on-line safety and know what to do in the case of an incident.
- A planned online safety curriculum is provided as part of Computing and PHSE and is regularly revisited.
- Pupils are taught to be aware of the materials / content they access on-line and are guided to validate the accuracy of information and respect copyright when using material accessed on the internet.
- Digital leaders support the teaching of online safety across the school and take part in the family of school online safety events.
- Safer Internet Day is celebrated across the school with a range of activities to raise the profile of online safety.
- In lessons where internet use is pre-planned, sites are pre-checked for content.
- Staff receive regular updates on current online safety issues as well as formal training through the Local Authority.
- The school provides appropriate online safety information to parents and carers via the learning platform and parent events.

4. Communications

- The school email and Tucasi are used for communications. The use of personal email addresses, text messaging or social media is not permitted to communicate to parents or pupils.
- Digital communication by all staff, governors and other users is professional in tone and content. Staff are not expected to reply out of school hours.
- Pupils are taught how to communicate appropriately with each other and not to communicate with anyone outside of the school community. They are regularly reminded of their obligations under the AUP.

- Personal information is not posted on the school website or associated school websites (e.g. PTA website) and only official email addresses should be used to identify members of staff.

5. Social Media

- Social networking sites are not to be accessed from school equipment.
- Where staff use social media, they must not mention Bramhope Primary School in name or implicitly or share information relating to school directly or indirectly on social media.
- No reference is made in personal social media to students / pupils, parents / carers or school staff.
- Bramhope Primary School will monitor the Internet for public postings about the school.

6. Digital Imagery

- All digital images are saved in the designated staff drive. Digital images are not kept on staff or pupil laptops.
- Staff will educate pupils about the risks of taking and sharing digital images as well as an understanding of copyright.
- Written permission from parents or carers is obtained before pupils appear on the school website, newsletter and learning platform or twitter account and before any pupil personal data is passed on to any on-line third party educational provider.
- Parents are reminded that they may take photos / videos of their own children at school events but that these must not be shared on social media where other children are included in the photo / video.
- Staff are allowed to take educational photos but these are only taken on school devices.
- When taking digital / video images, pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Pupils' full names are not used anywhere on a school website, twitter or blog, particularly in association with photographs.

7. Remote Learning

- Remote learning must follow guidelines issued in the remote learning policy (October 2020). These include actions such as: attendance, supervision, appropriate dress, guidance around appropriate communication. Please see full guidance for parents and staff in remote learning policy.
- ·Remote learning must also maintain the same child protection and safeguarding protocols that apply in the normal school environment including the staff and parent/pupil acceptable use policies.
- The SLT will be responsible for monitoring the security of remote learning systems, including data protection and safeguarding considerations with I.T support.

8. Incidents / Breach Of The Policy

- All incidents are dealt in accordance with the online safety incident flow chart (Appendix 1) 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.
- All incidents are documented on the Online Safety Incident Log in Appendix 2. In addition, if the safety incident is a safe guarding incident, a cause for concern form will be completed. This log of incidents is shared with governors at each meeting.
- 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.

9. Roles And Responsibilities

- The Head Teacher is responsible for reviewing filter reports and putting into place action required following any incidents as well as reviewing any online incidents and reporting these back to governors.
- The deputy designated safeguarding lead is responsible for ensuring the filtering system is compliant with LEA guidelines and the testing of the system.
- The Computing Subject Coordinator is responsible for the delivery of online safety within the computing curriculum and the updates of policy and AUP documentation.
- The school designated technician is responsible for the upkeep and security of the school network in line with this policy.
- Reception staff are responsible for ensuring all supply staff have a correct supply teacher log on and are reminded not to use mobile phones around children in school.
- All school staff, pupils and parents are responsible for ensuring they meet the requirements of the relevant AUPs.
- All school staff, pupils and parents are responsible for notifying any safety breach to the Head Teacher.

10. Ownership Of Policy And Review

This policy has been written by the following working group:

- The Headteacher – Mrs R. Colbourn
- Computing Coordinator – Mrs C. Hahnel
- Governor representation: - TBC
- Parent representative – TBC

It was reviewed and approved by school governors in July 2018.
The policy will be reviewed in May 2020

Appendices

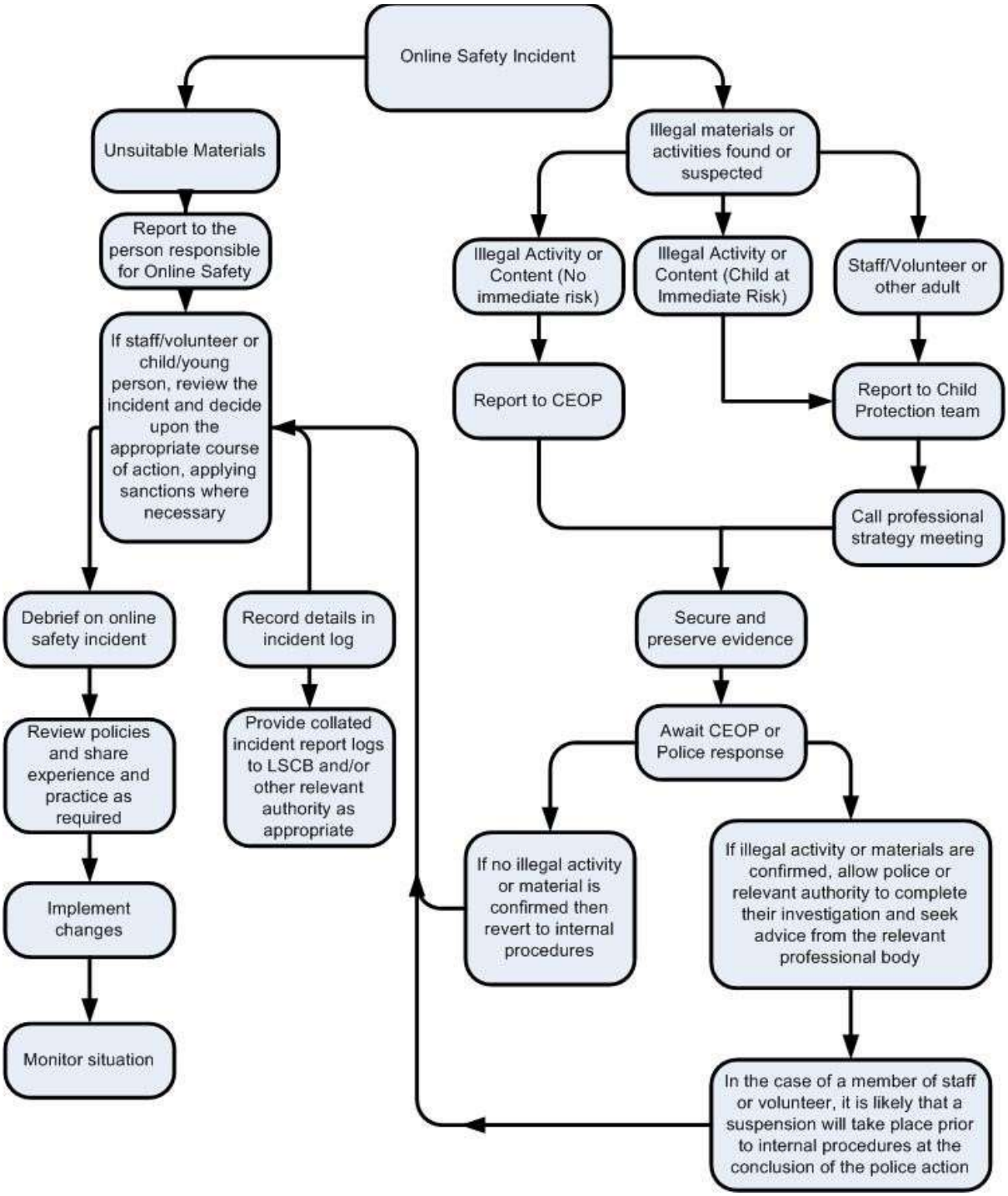
Appendix 1 - **Dealing with online safety incidents**

Appendix 2 - **Online safety incident log**

Appendix 3 - **Filtering monitoring log**

-

Appendix 1 **Dealing with online safety incidents**



-

Appendix 2 **Online safety incident log**

ONLINE SAFETY INCIDENT LOG – Bramhope Primary School						
Date	Time	Incident	**Action Taken**		**Reported By**	**Signature**
			What?	By Whom?		

-

Appendix 3 **Filtering monitoring log**

FILTER MONITORING LOG – Bramhope Primary School						
Date	Time	Word / Phrase Searched	Name of User	Outcome	Action Required	Action Complete (date and signature)

-