Castle Hill Primary School
Online Safety Policy

Reviewed and Updated:
1.11.20

Looked over on:
17.11.26

Appendices

Appendix	
1	Online Safety Incident Flowchart
2	School Technical Security Overview
3	AUP documents – Staff / Pupils / Visitors
4	Online Incident Report Log
5	School Data protection Policy – Castle Hill

Scope of the Policy

The regulation and use of technical solutions to safeguard children are important but must be balanced with teaching the necessary skills to enable pupils to take responsibility for their own safety in an ever changing digital world. The National Computing Curriculum states that children should be able to use technology safely, respectfully, and responsibly keeping personal information private, recognise acceptable or unacceptable behaviour and identify a range of ways to report concerns about content and contact. Children's safety is paramount and they will receive the help, guidance and support through the whole curriculum to enable them to recognise and avoid online risks and to build their resilience. During the delivery of the curriculum staff will reinforce and consolidate safe online learning

This policy applies to all members of the school community who have access to and are users of school ICT systems and online resources, both in and out of school.

The school will deal with incidents as outlined within this policy, within the remit of their safeguarding, behaviour and anti-bulling policies (and others when applicable).

Development of the Policy

This Online Safety Policy has been developed by a working party led by Bolton Schools' ICT. It is recommended that this Policy is reviewed and ratified by the school's own relevant parties* i.e.

- Headteacher
- Governing Body

This Online Safety Policy was approved by the Governing Body *on:*	November 2020

Schedule of Monitoring and Review

The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new Online threats or incidents that have taken place.	1.11.20
The implementation of this Online Safety Policy will be monitored by the:	Headteacher Governors Safeguarding Lead
The school will monitor the impact of the policy using:	Logs of reported incidents Monitoring logs of internet activity (including sites visited) Internal monitoring data for network activity
Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group at regular intervals:	Termly where appropriate

* In this policy whenever the term 'relevant parties' is used, school need to nominate who is responsible from this list

Should serious Online incidents take place, the following external persons / agencies should be informed:	Headteacher School Safeguarding Lead LADO Police **See Appendix 1**

Roles and Responsibilities

Headteacher:

The Headteacher has a duty of care for ensuring the day to day safety (including Online) of all members of the school community.

The role of the Headteacher will include:

- ensuring that all members of the school community understand and acknowledge their responsibilities in the event of a serious online allegation being made (**Appendix 1**)
- ensuring that all relevant staff receive suitable training to enable them to carry out their safeguarding responsibilities within the remit of the Online Safety Policy
- ensuring that the Online Safety Policy is accessible to the wider School Community (School website)
- meeting at regular intervals with the Computing Lead to ensure the implementation of this policy (as outlined above). It is recommended that regular subject leader time is allocated to fulfil the role
- ensuring the relevant parties receive regular monitoring reports from the Computing lead
- ensuring there are opportunities to communicate up to date Online Safety information to the wider school community

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Anti-Bullying and Behaviour Policy.

Governors:

Governors are responsible for the approval of this Online Safety Policy and for reviewing its effectiveness. This will be carried out by the Governing board, receiving regular information about online incidents and monitoring reports.

Where appointed, the role of the Safeguarding Governor will include:

- regular meetings with the Computing lead/team
- regular monitoring of the Online Incident Log/CPOMS** (which will include anonymous details of Online Incidents Report Log **appendix 4**)
- ensuring robust technical support is in place to keep systems safe and secure
- regular monitoring of filtering
- reporting to the Governing board
- attending training for online safety where appropriate

Safeguarding Lead

The Safeguarding Lead is responsible for taking any necessary action as per the Online Safety Incident reporting flowchart (**Appendix 1**).

** If a school is using CPOMS it is important to ensure that the lozenges are set up to be specific and appropriate, for example – PEGI, Snapchat, Instagram etc. This will assist in collating and responding to Online Incidents.

They will be trained in online issues and acknowledge and understand the potential for serious child protection / safeguarding issues that arise from, but not limited to

- sharing of personal data
- accessing illegal / inappropriate materials
- exposure to inappropriate online content
- inappropriate contact with adults/strangers
- potential or actual incidents of grooming
- sexting
- cyber-bullying

In the event of a child protection or safeguarding incident pertaining to the above, the safeguarding lead will refer to appendix 1.

Computing Lead / Team

The Computing Lead / Team is responsible for the management of online issues and take a leading role in establishing and reviewing the school Online Safety Policy.
The role of the Computing Lead/team includes:

- providing advice for staff and signpost relevant training and resources
- liaising with relevant outside agencies
- liaising with relevant technical support teams
- collating and reviewing reports of Online Incidents (A**ppendix 4 / CPOMS**)
- meeting regularly with Headteacher and relevant parties to discuss issues and subsequent actions
- taking action in response to issues identified
- communicating up-to-date Online Safety information to the wider school community

School Staff

It is essential that all staff

- understand and acknowledge their responsibilities as outlined in this Policy
- have read, understood and signed the Staff Acceptable Use Policy (Appendix 3)
- keep up to date with the Online Safety Policy as part of their CPD
- have an up-to-date awareness of online matters pertinent to the children that they teach/have contact with
- report concerns and log incidents (A**ppendix 4** / CPOMS**)
- when addressing any suspected misuse or Online Safety Issue, refer to appendix 1 or appendix 4, depending on the severity
- ensure that all digital communications with the School Community are on a professional level and only carried out using official school approved systems
- apply this Online Safety Policy to all aspects of the Curriculum
- share, discuss and ensure the children understand and acknowledge their responsibility to follow their age-appropriate Acceptable Use Policy
- are good role models in their use of all digital technologies
- are vigilant in monitoring how pupils use digital technologies and access online content whilst in their care

It is accepted that from time to time, for purposeful/appropriate educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable with clear reasons for the need.

Technical support

The school's technical infrastructure must be secure and actively reduces the risk of misuse or malicious attack.
To facilitate this, school has purchased support from Bolton Schools ICT.
The role includes:

- ensuring that detected risks and/or misuse is reported to the Headteacher at school
- ensuring that schools are informed of any changes to guidance or any planned maintenance
- school technical systems will be managed and reviewed annually in ways that ensure that the school meets recommended technical requirements
- all users will have clearly defined access rights to school technical systems and devices
- all school network users will be assigned an individual username and password at the appropriate level of access needed for their role
- ensuring internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list
- content lists are regularly updated and internet use is logged and regularly monitored
- there is a clear process in place to deal with requests for filtering changes
- provide a platform where school should report any content accessible in school but deemed inappropriate
- ensuring 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 (**Appendix 2**)

Pupils

The children's learning will progress through a broad, effective and relevant Online Safety curriculum.
A pupils learning journey will be holistic in that it will include, but is not limited to their online reputation, online bullying and their health and wellbeing.

It is essential that all pupils should:

- understand, acknowledge and adhere to their age-appropriate Acceptable Use Policy (**Appendix 3**)
- be able to recognise when something makes them feel uncomfortable (butterfly feeling) and know how to report it
- accept their responsibility to respond accordingly to any content they consider as inappropriate
- understand the importance of being a responsible digital citizen and realise that the school's Online Safety Policy applies to their actions both in and out of school
- know that school will take action in response to any breach of the Online Safety Policy

Parents / Carers / Responsible adults

Parents play an essential role in the education of their children and in the monitoring / regulation of the children's on-line usage. Due to the ever evolving Digital World, adults can sometimes be unsure of how to respond to online risks and issues. They may also underestimate how often pupils encounter potentially harmful and inappropriate online material.
Therefore, it is essential that all adults should:

- promote safe and responsible online practice and must support the school by adhering to the school's Safeguarding and Online Safety Policy in relation to digital and video images taken whilst on school premises or at school events
- understand, acknowledge and adhere to their child's Acceptable Use Policy (**Appendix 3**)

- understand, acknowledge and ensure that their child adheres to school procedure relating to their use of personal devices whilst on school grounds

To support the school community, school will provide information and awareness through, but not limited to:

- letters, newsletters, website links, publications, external agencies
- Parents / Carer workshops
- high profile events / campaigns e.g. Safer Internet Day

Visitors entering school

It is essential that school apprise visitors of all relevant policies pertaining to their visit and contact with pupils.

Useful Information

Safeguarding

In the event of a Safeguarding infringement or suspicion, appendix 1 must be followed with consideration of the following**:**

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported
- Conduct the procedure using a computer that will not be used by pupils and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the investigation, but also that the sites and content visited are closely monitored and recorded (to provide further protection)
- Record any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed and signed (except in the case of images of child sexual abuse – see below)
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include: incidents of 'grooming' behaviour the sending of obscene materials to a child adult material which potentially breaches the Obscene Publications Act criminally racist material other criminal conduct, activity or materials. Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the relevant group for evidence and reference purposes.

Data Protection

Personal and sensitive data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. Schools are audited regularly regarding how they handle their data, for further information please refer to school Data Protection Policy (**Appendix 5**).

Communications

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

- The Office 365 school email service is safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school
- When accessing emails out of the schools setting, staff will only be able to access their schools emails using Microsoft Multifactor Authentication app.
- Users must immediately report, to the nominated person – in accordance with the school policy, 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.
- Any digital communication between staff and pupils or parents / carers (email, chat) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about online 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 website and only official email addresses should be used to identify members of staff.

Social Media

The school's use of social media is to promote the ethos of the school. It is the responsibility of all staff to ensure that the content they upload is for professional purposes only, be compliant with the school policies and protect the identity of pupils.