Hartlebury Church of England (Voluntary Controlled) Primary School

ONLINE SAFETY POLICY SEPTEMBER 2018

Ratified by Governing Body on: Wednesday 3rd October 2018

Next review date: October 2019

Our Core Christian Values

- **Love-** We care for everyone and everything in our community
- **Tolerance-** We value and accept everyone in our community; listening to their opinions and points of view.
- **Forgiveness-** There is nothing that cannot be put right.

Code of Conduct

- We tell the truth
- We respect all adults and children
- We allow others to learn without disruption or distraction
- We behave in a way that is safe for us and everyone around us
- We take care of our environment and the things in it.

Aims of this Policy

This policy has been written with consideration Keeping children safe in education Statutory guidance for schools and colleges September 2018 and The Education for the Connected World document.

All staff are trained annually in safeguarding children including the online safety element and have read and are aware of where to find Annex C of Keeping Children Safe in Education.

At Hartlebury Church of England (VC) Primary we are committed to ensuring that children learn how to use computers, ICT and modern technologies safely so that they:

- Are able to use ICT safely to support their learning in school
- Are able to use ICT and modern technologies outside school in a safe manner, including using ICT as a tool for communication
- Are prepared for the constant changes in the world of technology and understand how to use new and emerging technologies in a safe manner
- Know how to safeguard themselves online

This policy outlines the steps the school takes to protect children from harm when using ICT and also how the school proactively encourages children to develop a safe approach to using ICT whether in school or at home.

(See also appendix 3 – Incident work flow)

The Law

Our Online safety Policy has been written by the school, using advice from HCC and government guidance. The Policy is part of the school's Strategic Development Plan and related to other policies including Positive Learning, Safeguarding and behaviour management.

Data Protection policies.

As legislation is often amended and new regulations introduced the references made in this policy may be superseded. For an up to date list of legislation applying to schools please refer to the Department for Education website at

www.education.gov.uk/schools.

Roles and Responsibilities

The Headteacher, alongside the online safety office (Rebekah Salter) will:

- Ensure the policy is implemented, communicated and compliance with the policy is monitored
- Ensure staff training in online safety is provided and updated annually as part of safeguarding training
- Ensure immediate action is always taken if any risks or dangers are identified i.e. reporting of inappropriate websites
- Ensure that all reported incidents of cyber bullying are investigated
- Ensure appropriate web filtering software is used to protect users from potentially damaging/offensive material

Teachers and Staff will:

- Keep passwords private and only use their own login details, which are stored securely.
- Monitor and supervise pupils' internet usage and use of other IT resources
- Adhere to the Acceptable Use Agreement
- Promote online safety and teach online safety units as part of computing curriculum
- Engage in online safety training
- Only download attachments/material onto the school system if they are from a trusted source
- When capturing images, videos or sound clips of children, only use school cameras or recording devices

It is essential that pupils, parents/carers and the public at large have confidence in the school's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of staff members and the reputation of the school and the SAET academy are safeguarded. In this context, staff members must be conscious at all times of the need to keep their personal and professional lives separate.

Governors will:

- Ensure that the school is implementing this policy effectively
- Adhere to the acceptable use agreement when in school
- Have due regard for the importance of online safety in school

Teaching and Learning

The school will actively teach Online safety at an age-appropriate level. The school follows a scheme of work for each year group covering: what should and shouldn't be shared online, password control and cyber bullying among other topics. Online safety will also be embedded throughout learning whenever children are using ICT in other lessons.

Monitoring safe and secure systems

Internet access is regulated by HCC supplied filtered broadband connection which blocks access to unsuitable websites. Antivirus software has been installed on all computers and is to be maintained and updated regularly. Staff passwords are changed regularly and must be strong passwords. Staff will take responsibility for safeguarding confidential data saved to laptops, i.e. use of strong passwords. If personal data has to be saved to other media, e.g. data sticks or CDs, it is to be encrypted or strong password protected. Staff with access to the ICT systems containing confidential and personal data are to ensure that such data is properly protected at all times.

Safe use of the Internet and Web Filtering

- All staff and pupils will have access to the internet through the school's network
- All staff, volunteers who have use of the school's IT equipment, must read and sign the Staff Acceptable Use Agreement.
- All children must read and sign the Pupil Acceptable Use Agreement.
- If a site containing inappropriate material is encountered, children must report it to an adult who will report it to the Headteacher to pass to HCC
- If an adult finds a site that they consider unsuitable they should report it to the Headteacher

The use of Email

All teaching and support staff are provided with a school email address. Staff should use this address when sending work-related emails All emails should be professional in nature and staff should be aware that all emails can be retrieved at a later date should this be necessary. Staff emails should never be used to forward 'chain' or 'junk' email. Staff should not communicate with pupils via email

The school website

- The school web site complies with statutory DFE requirements
- Images that include pupils will be selected carefully and only used if parents have given permission for such images to be posted on line. Social Networking, Social Media and Personal Publishing (blogging)

Staff private use of social media:

- No reference should be made in social media to students / pupils, parents / carers / school staff or issues / situations related to the school
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- Staff are not permitted to maintain a Social Media relationship with any pupil, current or alumni until such time that the pupil turns 18. The Use of Cameras, Video and Audio Recording Equipment Staff may only use the school's photographic or video devices to support school trips and curriculum activities. Photos should only be uploaded to the school system. They should never upload images to the internet unless specific arrangements have been agreed with the Headteacher or Deputy Headteacher, nor circulate them in electronic form outside the school. It is never acceptable to use photographic or video devices in changing rooms or toilets.

Personal mobile phones and mobile devices

- Use of mobiles is discouraged throughout the school, particularly in certain areas. The areas which should be considered most vulnerable include: toilets and changing areas, including where children change for swimming.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring at the direction of the head teacher.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

Management of online safety incidents

- There is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions; all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes; support is actively sought from other agencies as needed (i.e. MASH, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- The Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- We will immediately refer any suspected illegal material to the appropriate authorities

Working in Partnership with Parents

Parents' attention will be drawn to the online safety policy through the school newsletters, information evenings and on the school website.

Protecting School Staff

In order to protect school staff we require that parents do not comment on school issues or staff using social networking sites. Any concerns or complaints should be discussed directly with the school. The school will take action if there is evidence that inappropriate comments about staff have been placed on the internet in a public arena.

Safeguarding – scope of this policy

(See also Safeguarding and behaviour policies)

The Education and Inspections Act 2006 empowers the Head Teacher 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 safety 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 (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the schools

Behaviour Management Policy.

The school will deal with such incidents within this policy and associated behaviour and preventing-bullying policy and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that takes place out of school when reported in school.

Appendix 1: Pupil and Parent Acceptable Use Agreement

Appendix 2: Staff and Volunteer Acceptable Use Agreement and Policy

Appendix 3: Incident Workflow

Appendix 1

Hartlebury Church of England (VC) Primary ICT Pupil Acceptable Use Agreement and Online safety Rules

- I will tell an adult straight away if something on the computer has upset me or worried me so if I find anything or anyone online that makes me feel uncomfortable, unsafe or uneasy in any way, I will tell an adult immediately.
- I will be polite and friendly to everyone I speak to on the computer so I will make sure that all online contact with other children and adults is responsible, polite and sensible.
- I will only send pictures, videos or words that are kind and friendly so I will only upload or add images, video, sounds or text that are appropriate, kind and truthful and will not possibly upset someone.
- I will not tell anyone on the computer my name, how old I am or where I live so I will keep my personal details private when I'm online.
- I know that my teacher will always check to see if I am being friendly and sensible on the computer and the internet and they will speak to my parents and carers if I am not.
- I will behave sensible when I am on the computer because I am responsible for the way I behave online, and I know that these rules are to keep me safe.

Think before you click!

Dear Parent/ Carer

ICT, including the internet, email, digital and mobile technologies has become an important part of learning in our school. We expect all children to act safely and be responsible when using any ICT. Please read and discuss these Online safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact your class teacher.

Parent/ carer signature

We have discussed this and ……………………………………........(child name) agrees to follow the Online safety rules and to support the safe use of ICT at Hartlebury Church of England (VC) Primary .

Parent/ Carer Signature …….………………………………………………….

Class …………………………………. Date ………………………………

Appendix 2

Hartlebury Church of England (VC) Primary

Staff (and Volunteer) Acceptable Use Policy Agreement Template

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

The Acceptable Use Policy is linked to other policies as appropriate, e.g.

- Data Protection Policy
- Privacy Notices
- Freedom of Information Policy
- Freedom of Information Publication Scheme
- Staff Code of Conduct
- Safeguarding Children Policy

The following legal requirements considered in the formation of the Acceptable Use Policy:

- Data Protection Act 2018 & GDPR 2018
- The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018
- Human Rights Act 1998
- Freedom of Information Act 2000
- Defamation Act 2013

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the *school* will monitor my use of the school digital technology and communications systems.

- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school

- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

- I will immediately report any illegal, inappropriate or harmful material or incident; I become aware of, to the appropriate person.

I will be professional in my communications and actions when using *school* ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in school in accordance with the school's policies.

- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.

- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school*

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not use personal email addresses on the school ICT systems.

- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.

- I understand that data protection policy requires that any staff or student / pupil data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *school*

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors board and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

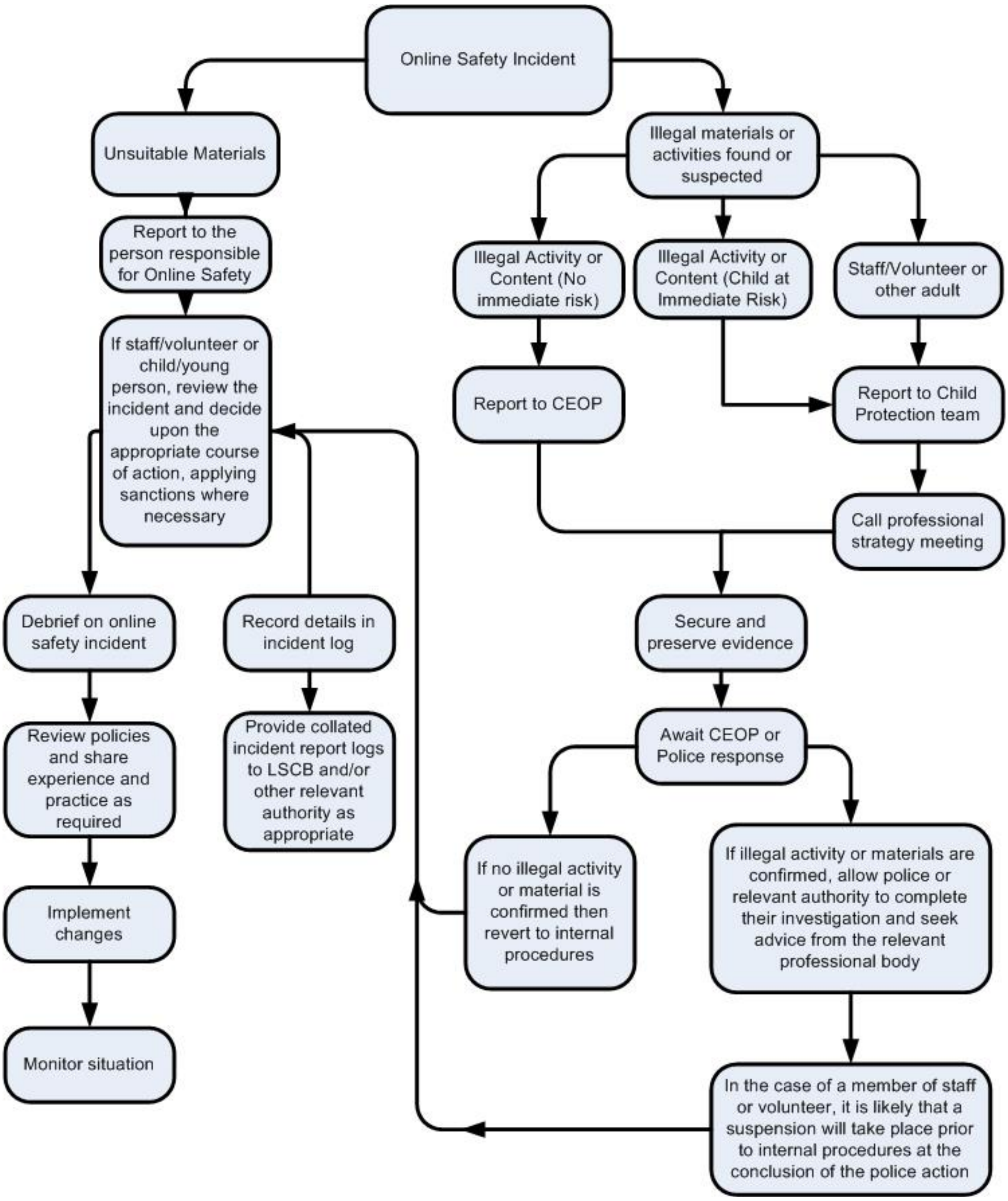
Staff / Volunteer Name: ....

Signed: ....

Date: ....

Appendix 3

Incident Workflow



Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action