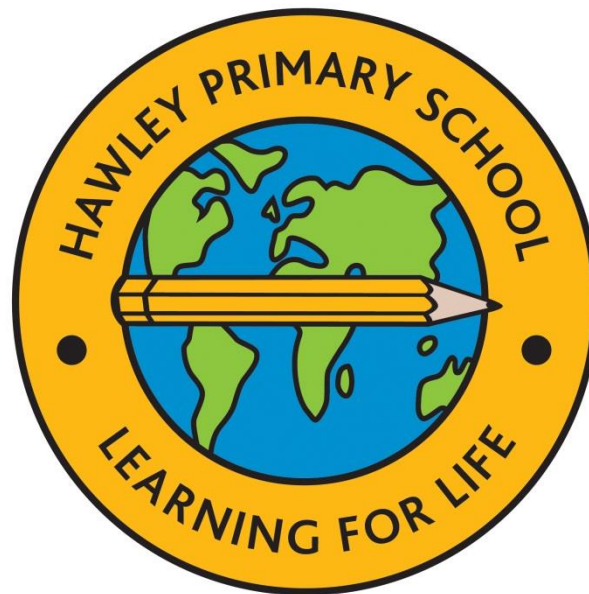


HAWLEY PRIMARY SCHOOL



E-SAFETY POLICY

AGREED BY GOVERNORS: Autumn 2021

LATEST REVIEW: Autumn 2021

NEXT REVIEW: Autumn 2023

Contents

1. Introduction and Overview

- a. E-Safety Explained
- b. Rationale and Scope
- c. Roles and Responsibilities
- d. Communication of Policy

2. Education and Curriculum

- a. Pupil E-Safety Curriculum
- b. Staff Training
- c. Governors Training
- d. Parent awareness and training

3. Conduct and Management

- a. Expected Conduct
- b. Handling Complaints
- c. Incident Management

4. Managing the Computing Infrastructure

- a. Internet access, security (virus protection), Network Management and filtering
- b. Passwords
- c. Email
- d. School Website
- e. Learning Platform
- f. Social Networking
- g. Video Conferencing

5. Equipment and Digital Content

- a. Personal mobile phones and devices
- b. Digital images and videos

6. Appendices

- a. Useful Links
- b. Acceptable Use Agreements
- c. Remote Learning Code of Conduct Contract

HAWLEY PRIMARY SCHOOL E-SAFETY POLICY

1 Introduction and Overview

1a. E-Safety Explained

Internet/online/cyber safety or E-Safety is trying to be safe on the internet and is the act of maximizing a user's awareness of personal safety and security risks to private information and property associated with using the internet, and the self-protection from computer crime.

1b. Rationale

At Hawley Primary School we believe that the Internet is an essential part of 21st century life for education, business and social interaction. In addition, the school has a duty to provide pupils with quality Internet access as part of their learning. This E-Safety Policy considers the use of both fixed and mobile internet, Virtual Learning Environments, PCs, laptops, I-Pads, webcams, digital video equipment, mobile phones, camera phones, personal digital assistants and portable media players. It will be revised to incorporate new and emerging technologies which will be examined for educational benefit and potential risks will be discussed with SLT before permission is given for use in school.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for students who show a responsible and mature approach to its use. We believe we have a duty to provide students with quality Internet access as part of their learning experience. Pupils also need to be able to evaluate Internet information and to take care of their own safety and security.

At Hawley Primary School we will endeavour to ensure that all members of the school community are aware of the E-Safety Policy and the implications for the individual. E-Safety depends on staff, governors, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication technologies.

Portable media may not be brought into school without specific permission and a virus check. Pupil access to the Internet will be by adult demonstration or directly supervised access to specific, approved on-line materials. Instruction in responsible and safe use by pupils will precede Internet access.

Our E-Safety Policy has been written by the school, agreed by the school leadership team and staff and approved by Governors. The E-Safety Policy and its implementation will be reviewed every three years. However, considering the ever-changing world of technology this policy may be reviewed at any other time appropriate to need.

Internet access in the school is provided via Hampshire County Council's IT department, HSPN. Filtering appropriate to the age of the pupils is provided as part of this link. A suitable virus protection system has been implemented through Hants IT and HSS (Hosted School Solutions). This virus protection system will be installed on all computers in school and automatically updated regularly.

The purpose of this policy is to:

- Set out expectations for all Hawley Primary School members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Safeguard and protect the children and staff of Hawley Primary School.
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
 - For the protection and benefit of the children and young people in their care.

- For their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice.
- For the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession.
- Set clear expectations of behaviour and codes of practice relevant to responsible use of the Internet for educational, personal, or recreational use.
- Help all participants to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary, or legal action will be taken.
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Establish clear structures by which online misdemeanors will be treated, and procedures to follow where there are doubts or concerns.

Scope

This policy applies to all members of the Hawley Primary School community (including staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of students / 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 e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

1c. Roles and Responsibility

Role	Key Responsibilities
<p>Head Teacher: Jane Baker</p>	<ul style="list-style-type: none"> • To take overall responsibility for e-safety provision. • Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the Designated Safeguarding team and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information. • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements. • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant. • To be aware of procedures to be followed in the event of a serious e-safety incident. • Liaise with the designated safeguarding team on all online-safety issues which might arise and receive regular updates on school issues. • To ensure that there is a system in place to support staff who carry out internal e-safety procedures. • Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding. • Ensure that policies and procedures are followed by all staff. • Undertake training in offline and online safeguarding. • Ensure the school implements and makes effective use of appropriate computing systems and services including school-safe filtering and monitoring and protected email systems. • Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles. • Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident. • Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety. • Ensure the school website meets statutory requirements. • Answer questions and/or address concerns raised by parents.
<p>E-Safety Co-ordinator / Designated Safeguarding Lead: Jane Baker</p>	<ul style="list-style-type: none"> • Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents. • Promotes an awareness and commitment to e-safeguarding throughout the school community. • Ensures that e-safety education is embedded across the curriculum. • Liaises with school ICT technical staff. • To communicate regularly with SLT and the designated e-safety Governor to discuss current issues, review incident logs and filtering. • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident. • To ensure that an e-safety incident log is kept up to date (CPOMS). • Facilitates training and advice for all staff. • Liaises with the Local Authority and relevant agencies.

	<ul style="list-style-type: none"> • Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: <ul style="list-style-type: none"> • sharing of personal data • access to illegal/inappropriate materials • inappropriate on-line contact with adults/strangers • potential or actual incidents of grooming • cyber-bullying and use of social media • Answer questions and/or address concerns raised by parents. <p>Key responsibilities (remember the DSL can delegate certain online-safety duties, e.g. to the online-safety coordinator, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education 2021):</p> <ul style="list-style-type: none"> • KCSIE makes clear that “the designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety) this lead responsibility should not be delegated.” • Work with the HT and technical staff to review protections for pupils in the home and remote-learning procedures, rules and safeguards. • Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL’s clear overarching responsibility for online safety is not compromised. • Ensure “An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.” • Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply. • Stay up to date with the latest trends in online safeguarding and “undertake Prevent awareness training.” • Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees. • Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident (CPOMS). • Facilitate training and advice for all staff, including supply teachers.
<p>Governing body, led by the E-safety governor:</p> <p>Ben O’Boyle</p>	<ul style="list-style-type: none"> • To ensure that the school follows all current e-safety advice to keep the children and staff safe. • To review the effectiveness of the E-Safety Policy. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities. <p>Key responsibilities (quotes are taken from Keeping Children Safe in Education 2021):</p> <ul style="list-style-type: none"> • Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board.

	<ul style="list-style-type: none"> • Ensure an appropriate senior member of staff, from the school leadership team, is appointed to the role of DSL [with] lead responsibility for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support. • Support the school in encouraging parents and the wider community to become engaged in online safety activities. • Have regular strategic reviews with the online-safety co-ordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings.
<p>Computing Leader:</p> <p>Hannah Taylor</p>	<ul style="list-style-type: none"> • As listed in the 'teachers and all staff' sections below. • Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum. • Work closely with the Designated Safeguarding Team, E-Safety Coordinator and all other staff. • Collaborate with technical staff and others responsible for computing use in school to ensure a common and consistent approach, in line with acceptable-use agreements.
<p>Data Manager/ Data Protection Officer</p> <p>Jane Baker</p>	<ul style="list-style-type: none"> • To ensure that all data held on pupils on the school office machines have appropriate access controls in place. • Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), especially this quote from the latter document: • "GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent (DPA, Part 2,18; Schedule 8, 4)
<p>All staff</p> <p>(Please See Staff List)</p>	<ul style="list-style-type: none"> • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy. • To embed e-safety issues in all aspects of the curriculum and other school activities. • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant). • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws. • To report any suspected misuse or problem to the e-safety coordinator promptly. • To read, understand and help promote the school's e-safety policies and guidance. • To be aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies with regard to these devices. • To report any suspected misuse or problem to the e-safety coordinator promptly. • To maintain an awareness of current e-safety issues and guidance e.g., through CPD. • To model safe, responsible, and professional behaviours in their own use of technology. • To ensure that any digital communications with pupils should be on a professional level and only through school-based systems, never through personal mechanisms, e.g., email, text, mobile phones etc.

	<ul style="list-style-type: none"> • Notify the DSL/E-Safety Coordinator if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon. • Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils). • Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures. • Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself. • Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place). • Prepare and check all online source and resources before using within the classroom. • Encourage pupils/students to follow their acceptable use policy, remind them about it and enforce school sanctions. • Notify the DSL/E-Safety Coordinator of new trends and issues before they become a problem. • Take a zero-tolerance approach to bullying/cyberbullying. • Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/E-Safety Coordinator know. • Receive regular updates from the DSL/E-Safety Coordinator and have a healthy curiosity for online safety issues. • Model safe, responsible, and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.
Pupils	<ul style="list-style-type: none"> • Read, understand, sign, and adhere to the Student / Pupil Acceptable Use Policy (NB: at KS1 it would be expected that parents / carers would sign on behalf of the pupils). • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • To understand the importance of reporting abuse, misuse, or access to inappropriate materials. • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and handheld devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • To help the school in the creation/ review of e-safety policies.

<p>Parents/carers</p>	<ul style="list-style-type: none"> • To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images. • Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it. • To access the school website / Seesaw / on-line student / pupil records in accordance with the relevant school Acceptable Use Agreement. • To consult with the school if they have any concerns about their children's use of technology. • Promote positive online safety and model safe, responsible, and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening, or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
<p>External groups</p>	<ul style="list-style-type: none"> • Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school. • Support the school in promoting online safety and data protection. • Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
<p>Network Manager/ technician:</p> <p>SchoolCare Technicians</p>	<ul style="list-style-type: none"> • To report any e-safety related issues that arises, to the e-safety coordinator. • To ensure that provision exists for misuse detection and malicious attack (e.g. keeping virus protection up to date). • To ensure the security of the school computing system. • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices. • That he / she keeps up to date with the school's e-safety policy and technical information to effectively carry out their e-safety role and to inform and update others as relevant. • That the use of the <i>network / Virtual Learning Environment / remote access / email</i> is regularly monitored in order that any misuse / attempted misuse can be reported to the <i>E-Safety Co-ordinator / Officer / Head teacher for investigation / action / sanction</i>. • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team. • Work with the Head teacher to ensure the school website meets statutory DfE requirements.

1d. **Communication of Policy**

This policy can only impact upon practice if it is a living document (regularly updated). It must be accessible to and understood by all members of Hawley Primary School. It will be communicated in the following ways:

- Posted on the school website
- Available on the internal staff network/drive (staff may print this if they prefer a paper copy)
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff)
- Integral to safeguarding updates and training for all staff (especially in Autumn Term refreshers)
- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders where possible, helping to ensure further engagement.

2 **Education and Curriculum**

2a. **Pupil E-Safety Curriculum**

The following subjects have the clearest online safety links:

- PSHE
- Relationships education, relationships and sex education (RSE) and health
- Computing
- Citizenship

However, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law. saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents. At Hawley Primary School all Staff will provide guidance to pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval, and evaluation. Parents will be informed that pupils will be provided with supervised Internet access. Staff will encourage children to use child safe search engines such as kiddle and swiggle.

Hawley Primary school:

- Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:
 - to STOP and THINK before they CLICK

- to develop a range of strategies to evaluate and verify information before accepting its accuracy;
 - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
 - to know how to narrow down or refine a search;
 - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
 - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
 - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
 - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
 - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
 - to understand why they must not post pictures or videos of others without their permission;
 - to know not to download any files – such as music files - without permission;
 - to have strategies for dealing with receipt of inappropriate materials;
 - [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
 - To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
 - To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e., parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
 - Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school/will be displayed when a student logs on to the school network.
 - Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.

- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include risks in pop-ups; buying on-line; on-line gaming / gambling;

2b. Staff Training

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy.

- A planned program of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction program, ensuring that they fully understand the school/academy online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead/ Designated Safeguarding Lead/ The Head Teacher will provide advice/guidance/training to individuals as required and/or requested.
- Staff should know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.

2c. Governors Training

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation.
- Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

2d. Parent Awareness and Training

Hawley Primary School:

- Endeavours to provide advice, guidance and training for parents (run by the online safety/designated safeguarding lead), including:
 - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
 - Information leaflets; in school newsletters; on the school web site;
 - Demonstrations, practical sessions/discussions held at school;
 - Suggestions for safe Internet use at home;
 - Provision of information about national support sites for parents.

A Parental consent form, which covers permission to access the Internet, will be issued to parents and carers at the beginning of the Autumn term, when their child begins school, to cover the forthcoming academic

years. This will contain the acceptable use guidelines and details of the school E-Safety Policy. Parents and carers will be required to sign the consent form and where appropriate, pupils will also be required to sign an acceptance of both the acceptable use guidelines and the E-Safety Policy. The signed consent form must be returned to the school for pupil access to the Internet to be permitted. Pupils will be informed that Internet use will be monitored. Pupil access may be withdrawn if the acceptable use guidelines are not adhered to. See Appendix 1 for useful resources for parents on E-Safety.

3 Conduct and Management

3a. Expected Conduct

At Hawley, all users:

- Are responsible for using the school Computing systems in accordance with the relevant Acceptable Use Policy.
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences.
- 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 e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Staff:

- Are responsible for reading the school's e-safety policy and using the school Computing systems accordingly, including the use of mobile phones, and hand held devices.
- Are responsible for following the rules set out in the Acceptable Use Policy.
- Are responsible for following the rules set out in the Remote Learning Code of Conduct Contract.

Students:

- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Should have a good understanding of how to be a good online digital citizen.
- Are responsible for following the rules set out in the Acceptable Use Policy.
- Are responsible for following the rules set out in the Remote Learning Code of Conduct Contract.

Parents/Carers:

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school.
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.
- Are responsible for following the rules set out in the Acceptable Use Policy.
- Are responsible for following the rules set out in the Remote Learning Code of Conduct Contract.

3b. **Handling Complaints**

- The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. **Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.**

- Staff and pupils are given information about infringements in use and possible sanctions.

Sanctions available include:

- o interview/counselling by teacher/Keystage Leader/E-Safety Coordinator/Headteacher;
- o informing parents or carers;
- o removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination work];
- o referral to LA/Police.

- Our E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy and Counter Cyber Bullying Policy. Complaints related to child protection are dealt with in accordance with school/LA child protection procedures.

3c. **Incident Management**

At Hawley Primary:

- There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions.
- Parents/carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship).

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the DSL to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets, and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

This school commits to take all reasonable precautions to ensure online safety but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact

on pupils when they come into school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes (CPOMS).

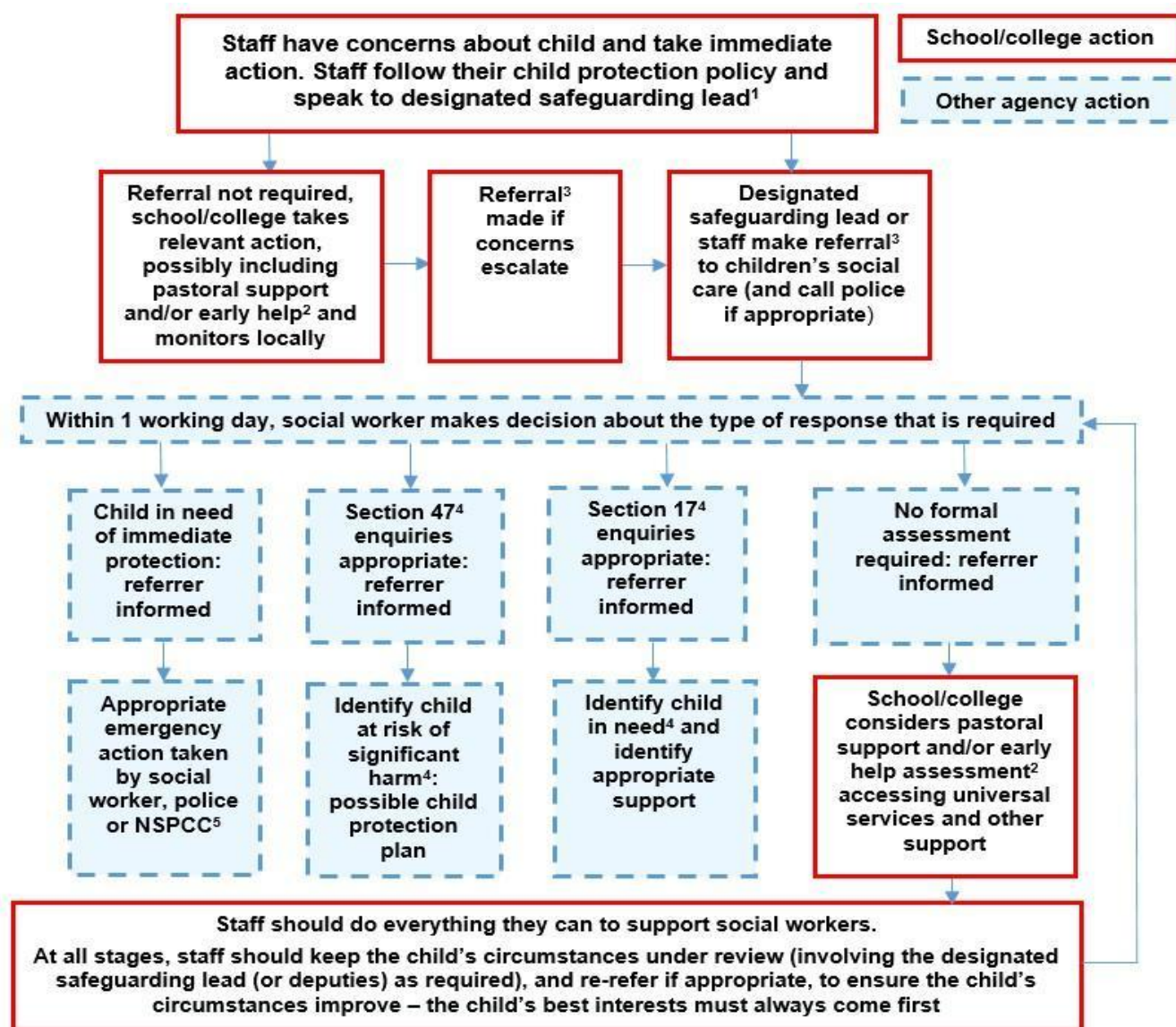
Any suspected online risk or infringement should be reported to the online safety lead/designated safeguarding team on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e. the local authority, UK Safer Internet Centre's Professionals' Online Safety Helpline, National Crime Agency, Prevent Officer, Police, Internet Watch Foundation).

Action Where There Concerns About a Child:

The following flow chart is taken from page 23 of Keeping Children Safe in Education 2021 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern. (All concerns should be logged on CPOMS)



4 Managing the Computing Infrastructure

4a. Internet Access, Security (virus protection), Network Management and Filtering

The security of the school information systems and Internet filtering will be reviewed regularly and is done in partnership with the LA. Virus Protection will be updated regularly. Personal data sent over the Internet will be encrypted or otherwise secured. Unapproved system utilities and executable files will not be allowed in pupils work areas or attached to e-mail.

Pupils are not allowed to download any files or programs without permission from a member of staff. Files held on the school's network will be regularly checked.

The IT Co-ordinator/network manager will review system capacity regularly. Any material that the school believes is illegal must be reported to appropriate agencies Edict, IWF or CEOP.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. Staff passwords are created by them and should never be divulged to anyone else. Staff laptops are a school resource and staff should exercise caution when downloading files. Staff should consult the network manager before downloading/installing programs.

4b. Passwords

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We advise staff to use STRONG passwords.
- We recommend for staff to regularly change their passwords.

4c. Email

Pupils at Hawley Primary School:

- May only use approved e-mail accounts on the school system as part of a class/group.
- Email accounts can only be set-up by the network manager with permission from the Head teacher.
- Will not have individual email accounts but use the internal messaging system as appropriately directed by their teachers.
- Must immediately tell a teacher if they receive offensive messages.
- Will not access their own private email accounts unless supervised by a teacher.

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper. The forwarding of chain letters is not permitted.

4d. School Website

The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. The website should comply with the DfE and school's guidelines on what should be published by a school on its website. The contact details on the website should be the school address, e-mail, and telephone number. Staff or pupils' personal information must not be published. Only the school admin e-mail or the headteacher@ address is given on the school's website site and HCC use spam filtering as our current domain host.

4e. **Learning Platforms**

- Photographs and videos uploaded to the schools learning platforms (Seesaw and Purple Mash) will only be accessible by members of the school community;
- In school, pupils are only able to upload items approved by a school staff member.
- Anything uploaded to the school learning platforms should follow the pupil's permissions e.g., photo permission.

4f. **Social Networking**

School staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or school staff.
- 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 or local authority.

HCC will block/filter access to social networking sites as far as possible e.g., Facebook, YouTube, Instagram, Twitter, TikTok and SnapChat. Pupils will not have access to social networking sites during school time.

Pupils will be taught never to give out personal details of any kind which may identify them and / or their location. Examples would include real name address, mobile or landline phone numbers, school attended, Instant Messaging (IM) and e-mail addresses, full names of friends, specific interests, and clubs etc.

Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. House number, street name or school.

Pupils will be advised on security and encouraged to keep passwords secret, deny access to unknown individuals, and instructed how to block unwanted communications. Students will also be advised not to publish specific and detailed private thoughts. Pupils will be advised to follow the Acceptable Use Policy.

4g. **Video Conferencing**

Safeguarding and child protection remains as important in this environment as anywhere else, and staff members should apply their school's safeguarding policies, guidance, and procedures to online learning, just as they would to classroom working - staff who are concerned about a child's welfare or have concerns for a child's safety should without delay, follow their school's safeguarding procedures.

All parties present should follow the Remote Learning Code of Conduct Contract.

The Head Teacher should provide clear guidelines for Video Conferencing. Any concerns should be taken immediately to the Head Teacher/ Designated Safeguarding Team.

5 Equipment and Digital Content

5a. Personal Mobile Phones and Devices

At Hawley Primary:

- Mobile phones brought into school are entirely at the staff member, pupils & parents' or visitors own risk. The school accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.
- Pupils are **not** allowed mobile phones/devices (e.g., smart watches) on the school premises.
- Staff members may use their phones out of teaching hours e.g., during school break times. Staff mobile phones should be kept out of sight of children where possible e.g., in the teacher's cupboard, bag, drawer. Staff members should keep their phones on silent (no vibration) or turned off.
- All visitors are requested to keep their phones on silent. Visitors should try to avoid using their mobile phones when children are present.
- All staff are governed by their contract of employment and the school's Acceptable Use Policy.
- The recording, taking, and sharing of images, video and audio on any mobile phones is prohibited.
- Parents/Carers are reminded regularly (e.g., annually or at the beginning of assemblies) about the importance of not sharing images or videos (e.g., of class performances) without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.
- If a member of staff breaches the school policy, then disciplinary action may be taken.
- In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Pupils' Use of Personal Devices

- Mobile devices are prohibited on the school premises.
- The school accepts that there may be circumstances in which a parent wishes their child to have a mobile phone for their own safety. Where this is the case, the school policy is that mobile phones should be brought to the school office and stored safely to be collected by the pupil at the end of the day.
- If a student breaches the school policy, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally owned devices and will be made aware of boundaries and consequences.

5b. Digital Images and Videos

At Hawley Primary:

- We gain parental/carers permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high-profile publications the school will obtain individual parental or pupil permission for its long term use;

- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

APPENDIX A - Helpful links

BBC Chat Guide

<http://www.bbc.co.uk/chatguide/>

Becta

<http://www.becta.org.uk/schools/esafety>

Childline

<http://www.childline.org.uk/>

Child Exploitation & Online Protection Centre

<http://www.ceop.gov.uk>

Grid Club and the Cyber Cafe

<http://www.gridclub.com>

Internet Watch Foundation

<http://www.iwf.org.uk/>

Internet Safety Zone

<http://www.internetsafetyzone.com/>

Kidsmart

<http://www.kidsmart.org.uk/>

NCH – The Children's Charity

<http://www.nch.org.uk/information/index.php?i=209>

NSPCC

<http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm>

Think U Know website

<http://www.thinkuknow.co.uk/>

Virtual Global Taskforce – Report Abuse

<http://www.virtualglobaltaskforce.com/>

Care for the family

www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf

Childnet International "Know It All" CD

<http://publications.teachernet.gov.uk>

Family Online Safe Institute

www.fosi.org

Internet Watch Foundation

www.iwf.org.uk

Parents Centre

www.parentscentre.gov.uk

How to report abuse, online for 8-10 year olds

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

Safer Internet Centre – <https://www.saferinternet.org.uk/>

Southwest Grid for Learning - <https://swgfl.org.uk/products-services/online-safety/>

Childnet – <http://www.childnet-int.org/>

Professionals Online Safety Helpline - <http://www.saferinternet.org.uk/about/helpline>

Revenge Porn Helpline - <https://revengepornhelpline.org.uk/>

Internet Watch Foundation - <https://www.iwf.org.uk/>

Report Harmful Content - <https://reportharmfulcontent.com/>

CEOP

CEOP - <http://ceop.police.uk/>

ThinkUKnow - <https://www.thinkuknow.co.uk/>

Others

LGfL – Online Safety Resources

Kent – Online Safety Resources page

INSAFE/Better Internet for Kids - <https://www.betterinternetforkids.eu/>

UK Council for Internet Safety (UKCIS) - <https://www.gov.uk/government/organisations/uk-council-for-internet-safety>

Netsmartz - <http://www.netsmartz.org/>

Tools for Schools

Online Safety BOOST – <https://boost.swgfl.org.uk/>

360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

360Data – online data protection self-review tool: www.360data.org.uk

SWGfL Test filtering - <http://testfiltering.com/>

UKCIS Digital Resilience Framework - <https://www.gov.uk/government/publications/digital-resilience-framework>

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) -

<http://enable.eun.org/>

SELMA – Hacking Hate - <https://selma.swgfl.co.uk>

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government - Better relationships, better learning, better behaviour -

<http://www.scotland.gov.uk/Publications/2013/03/7388>

DfE - Cyberbullying guidance -

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit:

<http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit>

Childnet – Project deSHAME – Online Sexual Harrassment

UKSIC – Sexting Resources

Anti-Bullying Network – <http://www.antibullying.net/cyberbullying1.htm>

[Ditch the Label – Online Bullying Charity](#)

[Diana Award – Anti-Bullying Campaign](#)

Social Networking

Digizen – [Social Networking](#)

UKSIC - [Safety Features on Social Networks](#)

[Children’s Commissioner, TES and Schillings – Young peoples’ rights on social media](#)

Curriculum

SWGfL Evolve - <https://projectevolve.co.uk>

[UKCCIS – Education for a connected world framework](#)

Teach Today – www.teachtoday.eu/

Insafe - [Education Resources](#)

Data Protection

[360data - free questionnaire and data protection self review tool](#)

[ICO Guides for Education \(wide range of sector specific guides\)](#)

[DfE advice on Cloud software services and the Data Protection Act](#)

[IRMS - Records Management Toolkit for Schools](#)

[NHS - Caldicott Principles \(information that must be released\)](#)

[ICO Guidance on taking photos in schools](#)

[Dotkumo - Best practice guide to using photos](#)

Professional Standards/Staff Training

[DfE – Keeping Children Safe in Education](#)

DfE - [Safer Working Practice for Adults who Work with Children and Young People](#)

[Childnet – School Pack for Online Safety Awareness](#)

[UK Safer Internet Centre Professionals Online Safety Helpline](#)

Infrastructure/Technical Support

[UKSIC – Appropriate Filtering and Monitoring](#)

[SWGfL Safety & Security Resources](#)

Somerset - [Questions for Technical Support](#)

NCA – [Guide to the Computer Misuse Act](#)

NEN – [Advice and Guidance Notes](#)

Working with parents and carers

[Online Safety BOOST Presentations - parent’s presentation](#)

[Vodafone Digital Parents Magazine](#)

[Childnet Webpages for Parents & Carers](#)

[Get Safe Online - resources for parents](#)

[Teach Today - resources for parents workshops/education](#)

[Internet Matters](#)

Prevent

[Prevent Duty Guidance](#)

[Prevent for schools – teaching resources](#)

[NCA – Cyber Prevent](#)

Childnet – [Trust Me](#)

Research

[Ofcom –Media Literacy Research](#)

Further links can be found at the end of the UKCIS [Education for a Connected World Framework](#)

APPENDIX B – ACCEPABLE USE AGREEMENTS



Staff/Governors

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with parents, pupils, and others, they are asked to sign this code of conduct. Staff should consult the detail of the school's Policy for Staff Acceptable Use of ICT for further information and clarification.

- I appreciate that ICT includes a wide range of system, including mobile phones, personal digital assistants, cameras, email, internet, and HCC intranet access and use of social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it may be a criminal offence to use the school ICT system for a purpose not permitted.
- I understand that I must not communicate information which is confidential to the school or which I do not have the authority to share.
- I understand that school information systems and hardware may not be used for personal or private without the permission of the Headteacher.
- I understand that my use of school information systems, internet and email may be monitored and recorded, subject to the safeguards outlined in the policy to ensure policy compliance.
- I understand the level of authority required to communicate with parents and pupils using the various methods of communication.
- I understand that I must not use the school ICT system to access inappropriate content.
- I understand that accessing, viewing, communicating, and downloading material which is pornographic, offensive, defamatory, derogatory, harassing or bullying is inappropriate use of ICT.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.
- I will not install any software or hardware without permission.
- I will follow the school's policy in respect of downloading and uploading of information and material.
- I will ensure that personal data is stored securely and is used appropriately whether in school, taken off the school premises or accessed remotely. I will not routinely keep personal data on removable storage devices. Where personal data is required, it will be password protected/encrypted and removed after use.
- I will respect copyright, intellectual property and data protection rights.
- I understand use for personal financial gain, gambling, political activity, advertising, or illegal purposes is not permitted.
- I will report any incidences of concern regarding children's safety to the Designated Safeguarding Lead or Headteacher.
- I will report any incidences of inappropriate use or abuse of ICT and inappropriate electronic communications, whether by pupils or colleagues, to the Headteacher, or if appropriate, the Chair of Governors.
- I will ensure that any electronic communication undertaken on behalf of the school, including email and instant messaging are compatible with my professional role and that messages do not present personal views or opinions and cannot be misunderstood or misinterpreted.
- I understand the school's stance on use of social networking and given my professional role working with children, will exercise care in any personal use of social networking sites.
- I will ensure that any electronic communications with pupils, where permitted, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

- I will promote e-safety with pupils in my care and help them to develop a responsible attitude to system use, communication and publishing.
- I understand that inappropriate use of personal and other non-school based ICT facilities can have implications for my employment at the school where this becomes known and where activities undertaken are inconsistent with expectations of staff working with children.

The school may exercise its right to monitor the use of the school's ICT systems and accesses, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's ICT systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, images or sound.

I have read and understand the Policy for Staff Acceptable Use of ICT and understand that inappropriate use may be misconduct or gross misconduct and may, after proper investigation, lead to a disciplinary sanction or dismissal. I understand that if I need any clarification regarding my use of ICT facilities, I can seek such clarification from any member of the Senior Leadership Team.

SIGNED:

DATE:.....

NAME (PRINT):



Foundation Stage / KS1

Home/School Acceptable Use of Technology Agreement

The Rationale for Technology at Hawley Primary School

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity, and raise awareness of context to promote effective learning. At Hawley Primary School we believe young people should always have an entitlement to safe internet access.

This Acceptable Use Agreement is intended to ensure:

- That our children use technology, including the internet, safely and responsibly inside and outside of school
- That our school systems and users are protected from accidental or deliberate misuse

At Hawley Primary School, we understand how important the use of technology is. The Internet and other technology can open up opportunities for everyone. We want to ensure that when you are using the internet, you are safe and the others around you are safe too.

So that I stay safe when I am using computers:

- I will ask an adult if I want to use the computers, laptops and iPads
- I will take care of the computer and other equipment I am using
- I will only use activities that an adult has told me or allowed me to use, making sure they are suitable for my age
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong
- I will tell an adult if I see something that upsets me on the screen
- I will tell an adult if someone tries to speak to me online
- I will only share my login details with my trusted adults at home or at school
- When online, I will not share my name, age, address, or school with anyone
- I know that if I break the rules, I might not be allowed to use a computer, laptop or iPad

Please sign your name below to show that you understand and agree to these rules.

Signed (child):

Signed (parent):



Key Stage 2

Home/School Acceptable Use of Technology Agreement



The Rationale for Technology at Hawley Primary School

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and raise awareness of context to promote effective learning. At Hawley Primary School we believe young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- That our children use technology, including the internet, safely and responsibly inside and outside of school
- That our school systems and users are protected from accidental or deliberate misuse

Acceptable Use of Technology - Policy Agreement

As a pupil at Hawley Primary School, I understand that I must use our 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.

For my own personal safety:

- I understand that the school will check my use of iPads, computers and laptops
- I will not share my username and password with anyone
- I will not write down my password
- I am aware of keeping safe online and I will only talk to people I know
- I will not share personal information about myself or others when on-line (this includes: names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If someone online asks to meet offline, I will tell an adult
- I will immediately tell an adult if I see any messages, photos, videos, pictures or words that make me feel uncomfortable

I understand that everyone has the right to use technology as a resource and:

- I understand that our school technology is for educational use
- I will not use school technology for personal reasons (online gaming, file sharing, or video broadcasting - YouTube) unless I have permission from an adult at school
- I will not download anything from the Internet without permission from an adult

I will act as I expect others to act towards me:

- I will respect others' work and property, will only access my own work and property and will not access another's work or property unless I have the owner's permission
- I will be polite and responsible when I communicate with others using technology
- I appreciate that others may have different opinions online and will respect them
- I will not take or distribute images of anyone without their permission
- I will only use appropriate language

The school has the responsibility to keep me safe when using:

Mobile devices

- I will not bring my mobile phone into school
- I will not use any personal device on school grounds. This includes **ANY** device that does not belong to school
- I understand that if am seen with a mobile device on school premises, it will be confiscated. My Parents will be asked to collect the device from my teacher
- Hawley Primary School does not accept responsibility for any mobile device brought into school.

School devices

- I will not upload, download or access any materials which are illegal or inappropriate
- I will immediately report any damage or faults involving equipment or software
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who has sent the email
- I will not install any programmes of any school device, nor will I try to alter computer settings

When using the internet for research or recreation, I recognise that:

- I will use quote marks to show where I have used someone else's words
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I will take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school has the right to take action against me if I am involved in incidents of inappropriate behaviour that are covered in this agreement when I am out of school and where they involve my membership of the school community. For example cyber-bullying, use of images or personal information.
- I understand that if I do not comply with this 'Acceptable Use Agreement', I may lose access to the school network, iPads and the internet.
- I understand that if I do not comply with this 'Acceptable Use Agreement' my Parents will be contacted and they may be asked to attend extra E-safety training and the Police may be involved as appropriate.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Home/School Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use of Technology Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school

Name of Pupil:

Class:

Signed:

Date:

Parent / Carer Countersignature.....

APPENDIX C – Remote Learning Code of Conduct Contract



Hawley Primary School cannot be held responsible for any incidents that occur if the code of conduct has not been followed.

Hawley Primary School – Remote Learning Code of Conduct Contract

As a school we will...	As a parent I will...	As I child I will...
<ul style="list-style-type: none"> Follow safeguarding procedures at all times to ensure learners are safe online. Provide online learning sessions that are appropriate and differentiated for children. Set work that is imaginative, engaging and appropriate across the whole curriculum. Offer support and help regularly throughout the school day. Be available to contact between the hours of 8am and 5pm. Support all learners and parents with online learning, where appropriate. Provide work that can be accessed by all. Communicate clearly the objectives and outcomes required from each lesson. Provide live teaching/video teaching sessions where appropriate. If learning from home, provide at least 3 pieces of work every day. Discuss roles and responsibilities with learners at the outset of all lessons. Reserve the right to remove students from the live sessions if we see/hear anything that does not follow the remote learning code of conduct. Endeavour to respond to queries as soon as possible. 	<ul style="list-style-type: none"> Understand that teachers are only available between 8am and 5pm. Understand that if my child is not in a live lesson, their teacher may not be able to respond immediately. Check my child's Seesaw account regularly to keep track of online sessions and learning. Be responsible for my child's Teams link. Not use Teams to create groups, initiate calls or meetings and ensure my child leaves Teams sessions when directed to. Be present in the room, or in the next room with the door open so I can see and hear everything that is happening during the live session. Not take any photos or recordings of online interactions/the live sessions in any way (including Seesaw, Teams and Purple Mash). Ensure that my communication in the online learning environment (e.g. Seesaw, Teams and Purple Mash) is always supportive and best for the learning and wellbeing of others. Ensure the environment is quiet, calm, safe and free from distractions. Ensure the background and foreground is appropriate and as neutral as possible (be mindful of what is visible to us). Ensure that anyone visible on the camera (at any time of the live session) is appropriately dressed. Ensure all that can be seen/heard act and speak in a courteous way at all times both to teachers/school staff and pupils. Understand that the teacher reserves the right to remove students from the live sessions if we see/hear anything that does not follow the remote learning code of conduct. Ensure that my child is safe online Support and encourage my child to participate in online learning. Ensure my child is present and on time for live lessons unless I have already informed the school of their absence. Communicate with teachers if my child is struggling/not able to access the work. Help my child to stick to a routine similar to the school day to support consistency. Encourage my child to try their best. Convey the importance of online learning to my child and praise my child for their work. 	<ul style="list-style-type: none"> Use only use Seesaw, Teams and Purple Mash as directed by my teacher. Only upload material that is related to my learning. Not use my Teams link to communicate with anyone other than my class teacher and ONLY when directed to do so by my teacher during live sessions. End Teams sessions when the teacher/school staff tells me to. Not take any photos or recordings of online interactions/the live sessions in any way (including Seesaw, Teams and Purple Mash). Ensure that my communication in the online learning environment (e.g. Seesaw, Teams and Purple Mash) is always supportive and best for the learning and wellbeing of others. Ensure the environment is quiet and free from distractions. Ensure the background and foreground is appropriate and as neutral as possible (be mindful of what is visible to us). Be punctual and appropriately dressed. Remain attentive and listen carefully to the school staff, following the school rules. Act and speak in a courteous way at all times both to teachers/school staff and pupils. Understand that the teacher reserves the right to remove me from the live sessions if we see/hear anything that does not follow the remote learning code of conduct. Understand that if I am not in a live lesson, my teacher may not be able to respond immediately. Complete my online learning every day, if I am learning from home. Tell an adult if I work is too easy or difficult. Take responsibility for my own learning and try my best during live lessons and with all the work I submit. Communicate appropriately in the chat function of the classroom. I will stay on mute unless my teacher asks me to turn my microphone on.
Class Teacher signed _____	Parent signed _____	Child signed _____