



# E-Safety Policy

**Hopewell School & motorvations@hopewell**

|                                    |               |
|------------------------------------|---------------|
| <b>Policy Date:</b>                | January 2021  |
| <b>Date Ratified by Governors:</b> | February 2021 |
| <b>Next Review:</b>                | January 2022  |

## Contents

### 1. Introduction and Overview

- Rationale and Scope
- Roles and responsibilities
- How the policy be communicated to staff/pupils/community
- Handling complaints
- Review and Monitoring

### 2. Education and Curriculum

- Pupil e-safety curriculum
- Staff and governor training
- Parent awareness and training

### 3. Expected Conduct and Incident Management

### 4. Managing the ICT Infrastructure

- Internet access, security (virus protection) and filtering
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
- School website
- Social networking
- Video Conferencing

### 5. Data Security

- Data transfer

### 6. Equipment and Digital Content

- Personal mobile phones and devices
- Digital images and video
- Asset disposal

### **Appendices:**

1. Acceptable Use Agreement (Staff)
2. Acceptable Use Agreement (Pupils) for KS2 and Secondary
3. Acceptable Use Agreement including photo/video permission (Parents)
4. Protocol for responding to e-safety incidents - handling infringements
5. Protocol for Data Security
6. Search and Confiscation guidance from DfE

## 1. Introduction and Overview

### Rationale

#### The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Hopewell School with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of Hopewell School.
- assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- 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.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

#### The main areas of risk for our school community can be summarised as follows:

### Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

### Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

### Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

## Scope

This policy applies to all members of Hopewell School community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of Hopewell School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-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. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

| Role  | Key Responsibilities  |
|---|---|
| Headteacher   | <ul style="list-style-type: none"> <li>• To take overall responsibility for e-safety provision</li> <li>• To take overall responsibility for data and data security (SIRO)</li> <li>• To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements</li> <li>• To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant</li> <li>• To be aware of procedures to be followed in the event of a serious e-safety incident.</li> <li>• To receive regular monitoring reports from the E-Safety Coordinator</li> <li>• To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. network manager)</li> </ul>   |
| Designated Safeguarding Leads: <ul style="list-style-type: none"> <li>• Susan Douglas HT</li> <li>• Rohan Cummings DHT</li> <li>• Nigel Bolitho Centre Manager motorvations</li> <li>• Nancy Bridge- Pupil Welfare</li> </ul> | <ul style="list-style-type: none"> <li>• 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/committee to discuss current issues, review incident logs and filtering / change control logs.</li> <li>• to ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident</li> <li>• to ensure that an e-safety incident log is kept up to date</li> <li>• facilitates training and advice for all staff</li> <li>• liaises with the Local Authority and relevant agencies</li> <li>• 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"> <li>○ sharing of personal data</li> <li>○ access to illegal / inappropriate materials</li> <li>○ inappropriate on-line contact with adults / strangers</li> <li>○ potential or actual incidents of grooming</li> <li>○ cyber-bullying and use of social media</li> </ul> </li> </ul> |

|   |  |
|---|--|
| <p>Governors/E-safety Governor<br/><b>(Robert Miller)</b></p> | <ul style="list-style-type: none"> <li>• To ensure that the school follows all current e-safety advice to keep the children and staff safe</li> <li>• To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor</li> <li>• To support the school in encouraging parents and the wider community to become engaged in e-safety activities</li> <li>• The role of the E-Safety Governor will include regular review with the E-Safety Co-ordinator (including e-safety incident logs, filtering / change control logs)</li> </ul>  |
| <p>Network Manager (<b>Iyke Eche</b>)</p>                     | <ul style="list-style-type: none"> <li>• To report any e-safety related issues that arises, to the e-safety coordinator.</li> <li>• To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed</li> <li>• To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date)</li> <li>• To ensure the security of the school ICT system</li> <li>• To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices</li> <li>• The school's policy on web filtering is applied and updated on a regular basis</li> <li>• Filtering issues are communicated to the e-safety governor.</li> <li>• That he keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant</li> <li>• That the use of the <i>network / remote access / email</i> is regularly monitored in order that any misuse / attempted misuse can be reported to the <i>E-Safety Co-ordinator/Headteacher for investigation / action / sanction</i></li> </ul> |
| <p>Teachers</p>   | <ul style="list-style-type: none"> <li>• To embed e-safety issues in all aspects of the curriculum and other school activities</li> <li>• To supervise and guide pupils carefully when engaged in learning activities involving online technology ( including, extra-curricular and extended school activities if relevant)</li> <li>• 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</li> </ul>   |

|                        |   |
|------------------------|---|
| <p>All Staff</p>       | <ul style="list-style-type: none"> <li>• To read, understand and help promote the school’s e-safety policies and guidance</li> <li>• To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy</li> <li>• 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</li> <li>• To maintain an awareness of current e-safety issues and guidance e.g. through CPD</li> <li>• To model safe, responsible and professional behaviours in their own use of technology</li> <li>• 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.</li> </ul>   |
| <p>Pupils</p>          | <ul style="list-style-type: none"> <li>• 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)</li> <li>• Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations</li> <li>• To understand the importance of reporting abuse, misuse or access to inappropriate materials</li> <li>• To know what action to take if they or someone they know feels worried or vulnerable when using online technology.</li> <li>• To know and understand school policy on the use of mobile phones, digital cameras and hand held devices.</li> <li>• To know and understand school policy on the taking / use of images and on cyber-bullying.</li> <li>• 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</li> <li>• To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home</li> <li>• To help the school in the creation/ review of e-safety policies</li> </ul> |
| <p>Parent/Carers</p>   | <ul style="list-style-type: none"> <li>• 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</li> <li>• To read, understand and promote the school Pupil Acceptable Use Agreement with their children</li> <li>• To access the school website in accordance with the relevant school Acceptable Use Agreement.</li> <li>• To consult with the school if they have any concerns about their children’s use of technology</li> </ul>   |
| <p>External groups</p> | <ul style="list-style-type: none"> <li>• Any external individual/organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school</li> </ul>  |

## Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website/staff room/classrooms.
- Policy to be part of school induction pack for new staff.
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school.
- Acceptable use agreements to be held in pupil and personnel files.

## 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. The school cannot 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:

- interview/counselling by tutor/E-Safety Coordinator/Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
- 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. Complaints related to child protection are dealt with in accordance with school child protection procedures.

## Review and Monitoring

The e-safety policy is referenced from within other school policies: Child Protection policy, Anti-Bullying policy, Behaviour policy and in the School Development Plan.

- The school has an e-safety coordinator who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The e-safety policy has been written by the school e-safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders such as the PTA. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

## 2. Education and Curriculum

### Pupil e-safety curriculum

This school

- Has a clear, progressive e-safety education programme as part of the Computing curriculum/PSHE curriculum. It is built on e-safeguarding and e-literacy framework for Y1 to Y11/national guidance. 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.
- 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 popups; buying on-line; on-line gaming/gambling;

### Staff training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on e-safety issues and the school's e-safety education program through termly annual meetings;
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies.

### Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, 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 held at school;
  - suggestions for safe Internet use at home;
  - provision of information about national support sites for parents.

## 3. Expected Conduct and Incident management

### Expected conduct

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (at KS1 it would be expected that parents/carers would sign on behalf of the pupils.)
- 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
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying Staff
- are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices. Students/Pupils
- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations 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

## **Incident Management**

In this school:

- 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.
- all members and its wider community 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 (e.g. UK Safer Internet Centre helpline) in dealing with e-safety issues.
- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders and Governors.
- 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.

## 4. Managing the ICT infrastructure

### Internet access, security (virus protection) and filtering

#### This school:

- Uses the Senso filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc.
- All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age/stage of the students;
- Ensures the network is healthy through use of ESET Endpoint Security and network set-up so staff and pupils cannot download and install executable files;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes/Internet Literacy lessons;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resources areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Requires staff to preview websites before use [where not previously viewed or cached] as a key way to direct students to age/subject appropriate web sites;
- Plans the curriculum context for Internet use to match pupils' ability, using childfriendly search engines where more open Internet searching is required; e.g. Yahoo for kids or Ask for kids , Google Safe Search , .....
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the e-safety Coordinator/*System administrator*. Our system administrator(s) logs or escalates as appropriate to the Technical service provider;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parent
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

## Network management (user access, backup)

This school:

- Uses individual, audited log-ins for all users;
- Uses teacher 'remote' management control tools for controlling workstations / viewing users/setting-up applications and Internet web sites, where useful;
- Has additional local network auditing software installed;
- Storage of all data within the school will conform to the UK data protection requirements;
- Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

### To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also *provide a different/use the same username and password* for access to our school's network;
- We provide pupils with an individual network log-in username.
- All pupils have their own unique username and password which gives them access to the Internet, *13+ pupils to have their own school approved email account*;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves. [Users needing access to secure data are timed out after 60 minutes and have to re-enter their username and password to re-enter the network.];
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day.
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus/spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional
- responsibilities and that they notify the school of any "significant personal use" as
- defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed;
- e.g. projector filters cleaned by site manager/TA; equipment installed and checked by approved Suppliers.

- Ensures that access to the school's network resources from remote locations by staff
- is restricted and access is only through school systems:
- *e.g. teachers access their area/a staff shared area for planning documentation via a VPN solution / RAV3 system;*
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
- Makes clear responsibilities for the daily back up of important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level
- /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security.

## Password policy

- 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 require staff to use STRONG passwords for access into our Network system.

## E-mail

### This school:

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example info@hopewellschool.co.uk or class e-mail addresses for communication with the wider public.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e-mails dangerous. We use desktop anti-virus product ESET Endpoint Security, plus direct email filtering provided by the google apps engine for viruses, Trojans and phishing.
- Finally, and in support of these, Draytek's GlobalView filtering monitors and protects
- our Internet access to the World Wide Web.

**Pupils:**

- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
- not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
- that an e-mail is a form of publishing where the message should be clear, short and concise;
- that any 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;
- they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;
- to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
- that they should think carefully before sending any attachments;
- embedding adverts is not allowed;
- that they must immediately tell a teacher/responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
- not to respond to malicious or threatening messages;
- not to delete malicious or threatening e-mails, but to keep them as evidence of bullying;
- not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
- that forwarding 'chain' e-mail letters is not permitted.
- Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

**Staff:**

- Staff can only use the school's Google Mail e-mail account on the school system
- Staff only use Hopewell Schools Google Apps e-mail systems for professional purposes
- Access in school to external personal e-mail accounts may be blocked
- Never use email to transfer staff or pupil personal data.
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
- the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
- the sending of chain letters is not permitted;
- embedding adverts is not allowed;
- All staff sign our School Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

## School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers: e.g. Headteacher
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. admin@hopewellschool.co.uk. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images;
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

## Social networking

- 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.
- 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
  - Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.



## 5. Data security: Management Information System access and Data transfer

### Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record in a spreadsheet.
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed:
  - staff,
  - governors,
  - pupils
  - parents
- This makes clear staffs' responsibilities with regard to data security, passwords and access.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal.
- We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email and network access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

## Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 60 minutes idle time.
- We use VPN solution with its 2-factor authentication for remote access into our systems.
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- Back-ups are encrypted. No back-up tapes leave the site on mobile devices.
- We use Veeam backup solutions for disaster recovery on our network.
- Paper based sensitive information is shredded, using cross cut shredder.
- We are using secure file deletion software.

## 6. Equipment and Digital Content

### Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, student's & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Student mobile phones which are brought into school must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day. Staff members may use their phones during school break times.
- All visitors are requested to keep their phones on silent.
- All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- 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.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Personal mobile phones will only be used during lessons with permission from the teacher.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- All mobile phones and personally-owned devices will be handed in at reception should they be brought into school.

### **Students' use of personal devices**

- The School strongly advises that student mobile phones and other digital devices, wearable technology including smart phones should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety. These must given in at the school entrance on arrival.
- 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 if they are taken in these circumstances.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- No students should bring his or her mobile phone or personally-owned device into school. Any device should be handed in on arrival. if student refused into school will be confiscated.

### **Staff use of personal devices**

- Staff handheld devices, including mobile phones and personal cameras must be noted in school – name, make & model, serial number.
- 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.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode and stored in the staff lockers during the school day. Personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the Head teacher and senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. 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.
- Staff will use a mobile application (What's App) for internal communications. Only members of staff are allowed in the communications group (closed and private) and this channel should only be used for school related messages. No pictures should be shared through this application

## Digital images and video

### In this school:

- We gain parental/carer 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;
- 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;
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- 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 Computing 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 identity 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.

## Asset disposal

Details of all school-owned hardware will be recorded in a hardware inventory. Details of all school-owned software will be recorded in a software inventory.

All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen

Disposal of any equipment will conform to [The Waste Electrical and Electronic Equipment Regulations 2006](#) and/or [The Waste Electrical and Electronic Equipment \(Amendment\) Regulations 2007](#). [Further information](#) can be found on the Environment Agency website.

# APPENDICES

# ***Hopewell School* eSafety**

## **Incident Log**

Log number:

| DATE  | TIME | NAME OF PUPIL, STAFF MEMBER OR PARENT/CARER | GENDER | ROOM | COMPUTER/ DEVICE NUMBER | NAME AND ROLE OF PERSON COMPLETING THIS ENTRY |
|---|------|---|--------|------|-------------------------|---|
| <b>DETAILS OF INCIDENT<br/>(including evidence)</b> |      |   |        |      |                         |   |
|   |      |   |        |      |                         |   |
| <b>ACTIONS AND REASONS</b>                          |      |   |        |      |                         |   |
|   |      |   |        |      |                         |   |

Details of ALL eSafety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Head teacher or Member of SLT.

| <b>RECORD OF REVIEWING DEVICES/INTERNET SITES (responding to incidents misuse)</b> |  |
|--|--|
| <b>Group</b>   |  |
| <b>Date</b>  |  |
| <b>Reason for investigation</b>  |  |

Any incidents involving Cyberbullying may also need to be recorded in the Bullying Incident Log

# ***Hopewell School* eSafety**

## **Incident Log**

| DETAILS OF FIRST REVIEWING |  |
|----------------------------|--|
| <b>Name</b>                |  |
| <b>Position</b>            |  |
| <b>Signature</b>           |  |

| DETAILS OF SECOND REVIEWING |  |
|-----------------------------|--|
| <b>Name</b>                 |  |
| <b>Position</b>             |  |
| <b>Signature</b>            |  |

| NAME AND LOCATION OF COMPUTER USED FOR REVIEW (for web sites) |
|---|
|   |

| WEB SITE(S) ADDRESS/DEVICE | REASON FOR CONCERN |
|----------------------------|--------------------|
|                            |                    |
|                            |                    |

| CONCLUSION | ACTION PROPOSED OR TAKEN |
|------------|--------------------------|
|            |                          |
|            |                          |

|                              |                        |
|------------------------------|------------------------|
| <b>Name of School</b>        | <b>HOPEWELL SCHOOL</b> |
| <b>Guidance review Date</b>  | <b>January 2021</b>    |
| <b>Date of next Review</b>   | <b>January 2022</b>    |
| <b>Ratified by Governors</b> | <b>February 2021</b>   |

### What do we do if...

**An inappropriate website is accessed unintentionally in school by a teacher or child.**

1. Play the situation down; don't make it into a drama.
2. Report to the head teacher/e- safety coordinator and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered.

**An inappropriate website is accessed intentionally by a child.**

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.

**An inappropriate website is accessed intentionally by a staff member.**

1. Ensure all evidence is stored and logged
2. Refer to the acceptable use and staffing policy that was signed by the staff member, and apply disciplinary procedure.
3. Notify governing body.
4. Inform the school technicians and ensure the site is filtered if need be.
5. In an extreme case where the material is of an illegal nature:
  - a. Contact the local police and follow their advice.

**An adult uses School IT equipment inappropriately.**

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the head teacher/e-Safety coordinator and ensure that there is no further access to the device. Record all actions taken.
3. If the material is offensive but not illegal, the head teacher should then:
  - Remove the device to a secure place.
  - Instigate an audit of all ICT equipment by the schools ICT managed service providers or technical teams to ensure there is no risk of pupils accessing inappropriate materials in the school.
  - Identify the precise details of the material.
  - Take appropriate disciplinary action (undertaken by Headteacher). ☐ Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature:
  - Contact the local police and follow their advice.
  - If requested to remove the device to a secure place and document what you have done.

All of the above incidences must be reported immediately to the head teacher, e-safety coordinator and child protection officer.

## E-safety Guidance

**A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.**

1. Advise the child not to respond to the message.
2. Refer to relevant policies including e-safety, anti-bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence through screenshots and printouts.
4. Inform the sender's e-mail service provider if known.

5. Notify parents of all the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform other agencies if required (LA, Child protection)

**Malicious or threatening comments are posted on an Internet site (such as social networking) about member of the school community (including pupils and staff).**

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at [ww.ceop.gov.uk/contact\\_us.html](http://www.ceop.gov.uk/contact_us.html).
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA and other agencies (child protection, etc.).

The school may wish to consider delivering a parent workshop for the school community

**You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites or gaming) to make inappropriate contact with the child**

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP <http://www.ceop.gov.uk/>
4. Consider the involvement police and social services.
5. Inform LA and other agencies.
6. Consider delivering a parent workshop for the school community.

**You are concerned that a child's safety is at risk because you suspect they are playing computer games that are inappropriate or certificated beyond the age of the the child**

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child and parents on appropriate games and content. You may want to use LGFL template letters to inform all or targeted parents.
3. If the game is played within school environment, ensure that the technical team block access to the game
4. Consider the involvement social services and child protection agencies.
5. Consider delivering a parent workshop for the school community.

**You are aware of social network posts and pages created by parents about the school. While no inaccurate information is posted, it is inflammatory and disruptive and staff are finding it hard not to respond.**

1. Contact the poster or page creator and discuss the issues in person
2. Provide central staff training and discuss as a staff how to behave when finding such posts and appropriate responses.
3. Contact governing body and parent association
4. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the head teacher, e-safety coordinator and child protection officer.

**Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.**

# HOPEWELL SCHOOL

## E-Safety agreement form for parents/carers

### Internet and ICT:

As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my daughter/son access to:

- the Internet at school
- the school's chosen email system
- the school's online managed learning environment
- ICT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's safety or e-behaviour they will contact me.

### Use of digital images, photography and video:

I understand the school has a clear policy on "The use of digital images and video" and I support this.

I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.

I accept that the school may use photographs/video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.

I will not take and then share online, photographs of other children (or staff) at school events without permission.

### Social networking and media sites:

I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.

**My daughter/son name(s):** \_\_\_\_\_

**Parent/guardian signature:** \_\_\_\_\_

**Date:** \_\_\_\_ / \_\_\_\_ / \_\_\_\_

## The use of digital images and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter/son.

We follow the following rules for any external use of digital images: If

**the pupil is named, we avoid using their photograph. If their photograph is used, we avoid naming the pupil.**

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staffs are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the Subject leader, Form tutor or teaching assistant) as part of a learning activity;  
e.g. taking photos or a video of progress made by a child, as part of the learning record, and then sharing with their parent/guardian.
- Your child's image being used for presentation purposes around the school:  
e.g. in class or wider school wall displays or PowerPoint® presentations.
- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;  
e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website.  
In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

**My daughter/son name(s):** \_\_\_\_\_

Parent/guardian signature: \_\_\_\_\_

Date: \_\_\_\_ / \_\_\_\_ / \_\_\_\_

## The use of social networking and on-line media

This school asks its whole community to promote the 3 commons approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

*How do we show common courtesy online?*

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

*How do we show common decency online?*

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

*How do we show common sense online?*

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site. *(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)* In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP report abuse process:

<https://www.thinkuknow.co.uk/parents/browser-safety/>

# HOPEWELL SCHOOL

|                        |                 |
|------------------------|-----------------|
| Name of school         | Hopewell School |
| AUP review date        | January 2021    |
| Date of next review    | Jan 2022        |
| Who reviewed this AUP? | Governing Body  |

## Acceptable Use Agreement:

### All Staff, Volunteers and Governors Agreement Form

Covers use of all digital technologies in school: i.e. e-mail, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I will follow the separate e-safety policy (including mobile and handheld devices).
- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access e-mail/Internet/Intranet/network or other school systems, *or any other school system I have access to.*
- I will ensure all documents, data etc., are printed, saved, accessed and deleted/shredded in accordance with the school's network/information security policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the school approved e-mail system(s)/*communication systems* for any school business, including communication with parents. This is: *WhatsApp, Google Hangouts and Google Mail*. I will only enter into communication regarding appropriate school business. Pupil pictures should not be taken/shared with WhatsApp.
- I will only use the school's approved systems: *Google Mail and Google Hangouts* to communicate with pupils, and will only do so for teaching & learning purposes.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or any filtering breach to Frederico Baroseiro (e-safety coordinator) or Rohan Cummings (Designated Child Protection Lead).
- I will report any equipment failure to Lyke Eche (Network Manager)

# HOPEWELL SCHOOL

- I will not download any software or resources from the Internet that can compromise the network or is not adequately licensed, or which might allow me to bypass filtering and security systems.
- I will check copyright and not publish or distribute any work, including images, music and videos, that is protected by copyright, without seeking the author's permission.
- I will not connect any device (including USB flash drives) to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's ESET Endpoint anti-virus and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will only use school approved equipment for any storage, editing or transfer of digital images/videos and ensure I only save photographs and videos of children and staff on the school approved system *or staff-only drive within school*.
- I will only use school approved systems to send and store files with pupil information. eg. reports, forms, risk assessments, etc.
- I will follow the school's policy on use of mobile phones/devices at school and only use during break times.
- I will use the school's Learning Platform in accordance with school protocols.
- I will ensure that any private social networking sites/blogs, etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, that I know how to use any social networking sites/tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities, and that I will notify the school of any "significant personal use", as defined by HM Revenue & Customs.
- I will only access school resources remotely (such as from home) using the School's secure VPN Connection and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption, and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information that is held within the school's information management system will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert the school's child protection officer/appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.

# HOPEWELL SCHOOL

- I will only use any other system I have access to in accordance with its policies.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff / named child protection officer at the school.
- I understand that all Internet usage and network usage can be logged, and that this information can be made available *to the Head/Safeguarding Lead* on their request.
- *Staff that have a teaching role only:* I will embed the school's e-safety/digital literacy curriculum into my teaching.

# HOPEWELL SCHOOL

## Acceptable Use Agreement Form: Staff, Volunteers, Governors

### User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and that I read and understand the school's most recent e-safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature

Date

Full Name

(printed)

Job Title / Role

### Authorised Signature (Head Teacher (Primary) / Head/Deputy/ Senior Teacher (Secondary))

I approve this user to be set-up on the school systems relevant to their role.

Signature

Date

Full Name

(printed)

## Think before you click

|  |  |
|--|--|
| <b>S</b>    | I will only use the Internet and email with an adult                     |
| <b>A</b>    | I will only click on icons and links when I know they are safe           |
| <b>F</b>   | I will only send friendly and polite messages                            |
| <b>E</b>  | If I see something I don't like on a screen, I will always tell an adult |
| My Name:   |  |
| My Signature:  |  |

# HOPEWELL SCHOOL

## KS2 Pupil Acceptable Use Agreement

*These rules will keep me safe and help me to be fair to others.*

1. I will only use the school's computers for schoolwork and homework.
2. I will only edit or delete my own files and not look at, or change, other people's files without their permission.
3. I will keep my logins and passwords secret.
4. I will not bring files into school without permission or upload inappropriate material to my workspace.
5. I am aware that some websites and social networks have age restrictions and I should respect this.
6. I will not attempt to visit Internet sites that I know to be banned by the school.
7. I will only e-mail people I know, or a responsible adult has approved.
8. The messages I send, or information I upload, will always be polite and sensible.
9. I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
10. I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
11. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher/responsible adult.

*I have read and understand these rules and agree to them.*

*Signed:*

*Date:*

# HOPEWELL SCHOOL

## KS3 Pupil Acceptable Use Agreement

*These rules will keep everyone safe and help us to be fair to others.*

1. I will only use the school's computers for schoolwork, homework and as directed.
2. I will not bring files into school (on removable media or online) without permission or upload inappropriate material to my workspace.  
I will only edit or delete my own files and not view, or change, other people's files without their permission.
3. I will keep my logins, IDs and passwords secret.
4. I will use the Internet responsibly and will not visit web sites I know to be banned by the school. I am also aware that during lessons I should visit web sites that are appropriate for my studies.
5. I will only e-mail people I know, or those approved by my teachers.
6. The messages I send, or information I upload, will always be polite and sensible.
7. I will not open attachments, or download a file, unless I have permission or I know and trust the person that has sent them.
8. I will not give my home address, phone number, send photographs or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
9. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless I take a trusted adult with me.
10. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will save it and talk to a teacher/trusted adult.
11. I am aware that some websites and social networks have age restrictions and I should respect this.
12. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.

I *have read and understand these rules and agree to them.*

*Signed:*

*Date:*

# HOPEWELL SCHOOL

## KS4 Pupil Acceptable Use Agreement

*These rules will keep everyone safe and help us to be fair to others.*

1. I will only use the school's computers for schoolwork, homework and as directed.
2. I will not bring files into school (on removable media or online) without permission or upload inappropriate material to my workspace.
3. I will only edit or delete my own files and not view, or change, other people's files without their permission.
4. I will keep my logins, IDs and passwords secret.
5. I will use the Internet responsibly and will not visit web sites I know to be banned by the school. I am also aware that during lessons I should visit web sites that are appropriate for my studies.
6. I will only e-mail people I know, or those approved by my teachers.
7. The messages I send, or information I upload, will always be polite and sensible.
8. I will not open attachments, or download a file, unless I have permission or I know and trust the person that has sent them.
9. I will not give my home address, phone number, send photographs or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
10. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless I take a trusted adult with me.
11. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will save it and talk to a teacher/trusted adult.
12. I am aware that some websites and social networks have age restrictions and I should respect this.
13. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.

I *have read and understand these rules and agree to them.*

*Signed:*

*Date:*