Hill Mead Primary School
E-Safety Policy
Spring 2019
E-Safety Policy 2018 - 2019

Hill Mead Primary

Contents

1. Introduction and Overview
   - Rationale and Scope
   - Roles and responsibilities
   - How the policy is communicated to staff, pupils and the community
   - Handling complaints
   - Review

2. Education and Curriculum
   - Pupil E-Safety curriculum
   - Staff training
   - Parents

3. Expected Conduct and Incident Management

4. Managing the IT Infrastructure
   - Internet Access, Security (Virus Protection) and Filtering
   - Network Management (user access, backup, curriculum and admin)
   - Passwords policy
   - Email
   - School website
   - Social Networking

5. Data Security
   - Management Information System Access
   - Data transfer
   - Asset Disposal

6. Equipment and Digital Content
   - Personal mobile phones and devices
   - Digital images and video

Appendices

1. Acceptable Use Agreement (Staff)
4. Acceptable Use Agreement (Pupils – All Other KS2)
5. Acceptable Use Agreement Including Photo/Video Permission (Parents of Digital Leaders)
6. Acceptable Use Agreement Including Photo/Video Permission (All Other Parents)
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 Hill Mead Primary School with respect to the use of digital technologies.
- Safeguard and protect the children and staff of Hill Mead Primary School.
- Assist school staff working with children to work safely and responsibly on 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 and/or suicide sites.
- Hate content.
- Content validation: how to check authenticity and accuracy of online content.

Contact:

- Grooming (sexual exploitation, radicalisation etc.)
- Cyberbullying in all forms.
- Social or commercial identity theft, including passwords.

Conduct:

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Health and wellbeing (amount of time spent online gambling, body image).
- ‘Sexting’ (the sending and/or 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), Ref Ofsted 2013.

Scope

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

The Education and Inspections Act 2006 empowers Head teachers to such an 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 / academy, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for policy). 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 anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

<table>
<thead>
<tr>
<th>Role</th>
<th>Key Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head Teacher</td>
<td>Full responsibility for e-safety provision</td>
</tr>
<tr>
<td><strong>Richard West</strong></td>
<td></td>
</tr>
<tr>
<td>E-Safety Lead</td>
<td>• To ensure that the e-safety policy becomes practice across the school</td>
</tr>
<tr>
<td><strong>Paul Highman, Senior Teacher</strong></td>
<td>To support the embedding of an e-safety culture within the curriculum</td>
</tr>
<tr>
<td>Designated Safeguarding Lead</td>
<td>To support teachers planning for e-safety awareness and practice</td>
</tr>
<tr>
<td><strong>Becky Lawrence</strong></td>
<td>To support the school in encouraging parents to become e-safety aware to ensure that their children are safe</td>
</tr>
<tr>
<td>Governors / E-Safety Governor</td>
<td>Elected annually</td>
</tr>
<tr>
<td>Network Manager / Technician</td>
<td>To report online safety related issues that come to their attention to the E-Safety Lead and Designated Safeguarding Lead</td>
</tr>
<tr>
<td><strong>London Connected Learning Centre</strong></td>
<td>To manage the school’s computer systems, ensuring</td>
</tr>
<tr>
<td></td>
<td>- school password policy is strictly adhered to.</td>
</tr>
<tr>
<td></td>
<td>- systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date)</td>
</tr>
<tr>
<td></td>
<td>- access controls/encryption exist to protect personal and sensitive information held on school-owned devices</td>
</tr>
<tr>
<td></td>
<td>- the school’s policy on web filtering is applied and updated on a regular basis</td>
</tr>
<tr>
<td></td>
<td>To keep up to date with the school’s online safety policy and technical</td>
</tr>
<tr>
<td></td>
<td>information in order to effectively carry out their online safety role and to update, inform and advise staff across the school</td>
</tr>
<tr>
<td></td>
<td>To ensure appropriate backup procedures and disaster recovery plans are in place</td>
</tr>
</tbody>
</table>
### Admins and Finance Officer
- To ensure that the data they manage is accurate and up-to-date
- Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements.
- The school is registered with the Information Commissioner
- To ensure all LGfL services are managed on behalf of the school, including maintaining the LGfL USO database of access accounts.

### Teachers
- 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 extracurricular 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.

### All Staff
- To read, understand and follow the school’s E-safety policy
- To report any suspected misuse or problem to the E-Safety Lead and Designated Safeguarding Lead.
- To maintain an awareness of current online safety issues and guidance
- To model safe, responsible and professional behaviours in their own use of technology

**Leaving the school as an employee**
- At the end of the period of employment to return any equipment or devices loaned by the school.
- All staff who have their school digital accounts deleted upon leaving. Emails will be re-directed to admin@hillmead.org

### Pupils
- Understand the school’s E-safety policy and follow the school’s guidance about acceptable use to keep safe online
- 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 understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school’s online safety policy covers their actions out of school

### Parents / Carers
- to support the school in promoting online safety and encourage their children to be safe online
- to consult with the school if they have any concerns about their children’s use of technology
- to raise any concerns they have regarding E-Safety
Handling Complaints:

- Hill Mead will take all reasonable precautions to ensure e-safety. However, owing to the global scale and linked nature of internet content, the availability of mobile technologies and the 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.

- If pupils misuse any digital technologies or deliberately cause others harm using digital technologies, there will be consequences in line with the school’s behaviour policy. The E-safety Lead and the Designated Safeguarding officer will consider any serious incidents and refer or seek advice from the Local Authority or the Police.

- Complaints or incidents of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with the school and Local Authority child protection procedures.

- All incidents will be recorded on CPOMs (the safeguarding recording and alert system)

- Any complaint about staff misuse is referred to the Head teacher and Designated Safeguarding Lead, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority’s Designated Officer).

Review:

The E-Safety Policy is reviewed annually by the E-Safety Lead, Designated Safeguarding Lead and Governing Body.

2. Education and Curriculum

Pupil E-Safety Curriculum:

Hill Mead Primary School:

- Promotes and implements an online safety education programme as part of the Computing curriculum and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience.
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- will remind students about their responsibilities in the digital world and how these keep them and others safe.
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright.
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.
• 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 online, online gaming and/or gambling.

Staff Training:

Hill Mead Primary 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.

• Provides training on e-safety education and implementation in the classroom with a focus on pupils understanding how they can keep themselves and others safe online.

• 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 Policy.

Parents:

Hill Mead Primary School:

• Shares good practice with parents through whole initiatives, class assemblies and events.

• Individual parents and carers are contacted when concern arise and are involved in follow-up actions.
3. Expected Conduct and Incident Management

Expected Conduct:

At Hill Mead Primary School, all users:

- Are responsible for using the school’s digital devices and systems in accordance with the E-Safety policy and understanding ‘acceptable use’ to keep themselves and others safe.
- Understand the importance of misuse or access to inappropriate materials and be aware of the consequences.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- 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.
- 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 cyberbullying.

All staff:

- Know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- Know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils.

Pupils:

- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents / Carers:

- Should know and understand what the ‘rules of appropriate use’ are at Hill Mead Primary School and what sanctions result from misuse.

Incident Management

In Hill Mead Primary School:

- When incidents occur a differentiated and appropriate range of sanctions is applied, 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. the local authority and regional broadband grid, UK Safer Internet Centre helpline, LGFL, CEOP) 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.
• Parents/carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
• Will contact the police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.
• We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing the ICT Infrastructure

Internet Access, Security (Virus Protection) and Filtering:

Hill Mead Primary School:

• Has the educational, filtered, secure broadband connectivity through the LGfL and so connects to the ‘private’ National Education Network.
• Uses the LGfL Net Sweeper 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 are 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 of pupils.
• Ensures the network is healthy through use of Sophos anti-virus software (from LGfL) and the network is set-up so staff and pupils cannot download executable files.
• Uses DfE, LA or LGfL approved systems such as S2S, USO FX, uses secured email to send personal data over the internet, and uses encrypted devices or secure remote access were staff need to access personal level data off-site.
• Blocks all chat rooms and social networking sites except those that are part of an educational network.
• Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons.
• Has blocked pupil access to shopping sites or to download music – except those approved for educational purposes at a regional or national level, such as Audio Network.
• Uses security time-outs on internet access where practicable / useful.
• Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.
• Is vigilant in its supervision of pupils’ use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
• Requires staff to preview websites before use (where not previously viewed or cached) and plan the curriculum context for internet use to match pupils’ ability, using child-friendly search engines where more open Internet searching is required, such as Google Safe Search.
• Informs staff and students that they must report any failure of the filtering systems directly to the London CLC System Administrator/E-safety Co-ordinators who will log or escalate as appropriate to the Technical Service Provider or LGfL Helpdesk as necessary.

• Provides advice and information on reporting offensive materials, abuse, bullying etc, and this advice is available for all pupils, staff and parents.

Network Management (User Access and Backup):

Hill Mead Primary School:

• Uses individual, audited log-ins for all staff users and group audited log-ins for all pupil users (by class).

• Uses guest accounts for external or short-term visitors for temporary access to appropriate services.

• Ensures the Systems Administrator / Network Manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies;

• Has daily back-up of school data (admin and curriculum);

• Storage of all data is secure and conforms to the UK data protection requirements and GDPR.

• 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, Hill Mead Primary School:

• Ensures staff access to the schools’ management information system is controlled through a separate password for data security purposes.

• Provides pupils with a year and class network log-in username and password, which gives them access to the internet.

• 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.

• Has set-up the network so that users cannot download executable files and/or programmes.

• Has blocked access to music/media download or shopping sites – except those approved for educational purposes.

• Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained and up to date and the school provides them with the information to do so.

• Maintains equipment to ensure Health and Safety is followed, e.g. equipment installed and checked by approved Suppliers / LA electrical engineers.

• Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, which complies with external Audit’s requirements.

• 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.

• Ensures our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use.

• Ensures all computer equipment is installed professionally and meets health and safety standards.

• Reviews the school ICT systems regularly with regard to health and safety and security.
Passwords Policy:

- All staff have their own unique username and private passwords to access school systems. This school advises staff to keep their password private, and must not leave it where others can find it.
- We recommend to staff to use STRONG passwords for access into our MIS system.
- We recommend to staff to change their passwords into the MIS, LGfL USO admin site, on a regular basis

Email:

Hill Mead Primary School:

- Provides staff with a Gmail account for their professional use and makes clear personal email should be through a separate account.
- Does not publish personal email addresses of pupils or staff on the school website. We use an anonymous email address, admin@hillmead.org, for communication with the wider public.
- Will contact the police if one of our staff receives an email that we consider is particularly disturbing or breaks the law.
- 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 emails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our internet access to the World Wide Web.

Staff:

- Staff use their school email for professional purposes only.
- Staff use a ‘closed’ email system which is used for LA communications and some ‘LA approved’ transfers of information.
- Never use email to transfer staff or pupil personal data (definition). We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer), Collect, and USO-FX.

School Website:

- The Head teacher takes overall responsibility to ensure that website content is accurate and that the quality of presentation is maintained.
- Uploading of information is restricted to our website authorisers: Kellaway Design Ltd.
- 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 and/or status.
- The point of contact on the website is the school address, telephone number and we use a general email contact address, admin@hillmead.org. Home information or individual email 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 when publishing to the school website.
• We do not use embedded geo-data in respect of stored images.
• Teachers use only school-approved, password protected blogging platforms for school blogs.

Cloud Environments
• Uploading of information on the schools’ online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
• Photographs and videos uploaded to the school’s online environment will only be accessible by members of the school community;
• In school, pupils are only able to upload and publish within school approved ‘Cloud’ systems.

Social Networking and Blogging:
• 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.
• Teachers are the gatekeepers to approve blogs to go live.
• Teachers will ensure blogs reflect school curriculum and the school teaching and learning principles.

School staff will ensure that in private use:
• No reference should be made in social media to 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 and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute.

Pupils:
• Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.

Parents:
• Are informed that they need to ask permission before uploading photographs, videos or any other information about other people.

CCTV:
• We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings, without permission, except where disclosed to the police as part of a criminal investigation.
5. Data Security: Management Information System Access and Data Transfer

Strategic and Operational Practices:
At Hill Mead Primary School:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who the main contact for key school information and the Information Asset Owner is the Head Teacher). Pupil and staff data is only accessed appropriately.
- We ensure staff know who to report any incidents to where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record in SIMS.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children’s Services / Family Services, Health, Welfare and Social Services.
- 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.
- 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.

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 10 minutes idle time.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use the Pan-London Admissions system (based on USO FX) to transfer admissions data.
- Staff with access to the Admissions system also use an LGfL OTP tag as an extra precaution.
- The schools systems cannot be accessed remotely.
- We use LGfL's USO to transfer other data to schools in London, such as references and reports of children.
- We use the LGfL secure data transfer system, USOAutoUpdate, for the creation of online user accounts for access to broadband services and the London content.
- 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.
- We use LGfL’s GridStore remote secure back-up / Jungle Disk and Amazon S3, for disaster recovery on our network / admin and curriculum server(s).
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted
data has been held and get a certificate of secure deletion for any server that once contained personal data.

- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.

- Paper based sensitive information is shredded, using cross cut shredder / collected by secure data disposal service.

- We are using secure file deletion software.

Asset Disposal:

- Details of all school-owned hardware is recorded in a hardware inventory.

- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item, as well as 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.


6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile phones brought into school are entirely at the staff members’, pupils’, 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.

Pupils’ Use of Personal Devices:

- The school only allows pupils who are home-alone (with signed parental permission) to bring their personal mobile phone to school. This is for the pupil’s own safety when travelling to and from school. Pupil mobile phones will be collected at the beginning of the day and stored in a secured location until the end of the day.

- The Bluetooth or similar function of a mobile device should be switched off at all times and not be used to send images or files to other mobile devices.

- If a pupil 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.

- Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
• 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.

Staff Use of Personal Devices:
• Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families in a personal capacity.
• Staff use personally-owned devices, such as mobile phones or, to record digital images and videos of pupils work for a range of learning and school purposes. All digital images and videos are deleted as soon as they have been used.

Storage, Syncing and Access
The device is accessed with a school owned account
• The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
• PIN access to the device must always be known by the network manager.

Digital Images and Video:
At Hill Mead Primary School:
• We gain parental/carers permission for use of digital photographs or video involving their child as part of the school agreement form when their child 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 or DVDs.
• If specific pupil photos (not group photos) are used on the school website, 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/filters 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 are 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
• 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 personal information public.
• 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.
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.

### Review of Policy

<table>
<thead>
<tr>
<th>Date agreed by governing body</th>
<th>Signature of Chair or Vice Chair</th>
</tr>
</thead>
<tbody>
<tr>
<td>6th February 2018</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date agreed for review</th>
<th>Frequency of Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autumn 2018</td>
<td>Annual (unless required earlier)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Responsibility for Review</th>
<th></th>
</tr>
</thead>
</table>