Haddenham St Mary's CE School

ONLINE SAFETY POLICY

Date agreed by Curriculum & Standards committee	**24 November 2025**
Date to be reviewed *(maximum* **36** *months after date above)*	**November 2028**
Date adopted by Governing Body	**10 February 2025**
Governors Committee accountable for review	**Curriculum and Standards**
Staff member accountable for review	**Designated Safeguarding Lead**
Governor accountable for monitoring	**Safeguarding Link governor**

Contents

Introduction and Overview

This policy applies to all members of Haddenham St Mary's CE School community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of the school's IT systems, both in and out of Haddenham St Mary's CE School. The policy should be read in conjunction with our Child Protection Policy and Staff Code of Conduct.

The policy takes account of Government legislation and guidance for the safe and secure provision of on-line education in school and remote education in the event of whole school Lockdown or individual classes or children sent home to self-isolate.

To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards which set out that schools and colleges should:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

All staff understand their role and responsibilities in relation to filtering and monitoring systems on the school IT network and on school devices, including using the reporting system to inform our IT provider and the DSL if they identify a concern in relation to inappropriate or harmful material being accessed in school:

DFE 'Teaching online safety in schools' *12th January 2023.*

https://www.gov.uk/government/publications/teaching-online-safety-inschools/teaching-online-safety-in-schools

'This non-statutory guidance outlines how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements. It complements existing subjects including:

- *Relationships Education*
- *Health Education*
- *PSHE*
- *Computing*

The guidance focuses on '*the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently*'

The teaching will be:

- Built into existing lessons across the curriculum – including Teach Computing Scheme and the PSHE Association Scheme
- Covered in specific on-line safety lessons
- Covered using school–wide approaches i.e. Anti-bullying week, Online Safety week, Healthy living week.

DFE 'The Coronavirus Act 2020 provision of remote Education (England) Temporary Continuity Direction' *30th Sept 2020* which sets out expectations in law for schools to

provide immediate access to quality remote education should pupils be sent home due to **public health measures**, such as isolation, bubbles being sent home, or local lockdowns.

'Remote education good practice' 1st Oct 2020

(https://www.gov.uk/government/publications/remote-education-good-practice)

Sets out advice and guidance on what matters most in remote education in particular when using online platforms.

The policy takes account of guidance in Keeping Children Safe in Education September 2025 on: Online safety and the awareness of the four areas of categorised risks (the 4 C's)

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

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact:** being subject to harmful online interaction with other users: for example: peer on peer abuse, commercial advertising and adults posing as young children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct:** personal online behaviour that increases the likelihood of, or causes harm; for example: making, sending and receiving explicit images and online bullying; and
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams

The purpose of this policy is to:

- Safeguard and protect the children and staff.
- Set out the key principles expected of all members of the school community at Haddenham St Mary's CE School, with respect to the use of IT-based technologies.
- Assist school staff to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with the school's anti-bullying and child protection 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.

Communication:

The policy is communicated to staff, pupils, parents, volunteers and visitors in the following ways:

- Policy is posted on the school website and in the staffroom.
- Policy is part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.

- Acceptable use agreements discussed with staff and pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, on entry to the school.

Reviewing and Monitoring Online Safety

- The online safety policy is referenced within other school policies including Child Protection policy, Anti-Bullying policy, Acceptable Use Policy and Data Protection Policy.
- The online safety policy will be reviewed every two years or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- filtering and monitoring logs of internet activity
- Surveys of parents/ carers, pupils and staff

Roles and responsibilities

Role	**Key Responsibilities**
Headteacher	• Takes overall responsibility for online safety provision • Is adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance • Leads a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • Takes overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice. • Ensures the school uses appropriate IT systems and services including, filtered Internet Service. • Is responsible for ensuring that all staff receive suitable online safety training • Ensures suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • Ensures Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • Ensure school website includes relevant online safety information.

Designated Safeguarding Officers	• Take day to day responsibility for online safety issues. Promote an awareness and commitment to online safety throughout the school community • Ensure that online safety education is embedded within the curriculum • Liaise with school technical staff where appropriate (computing lead. • Communicate regularly with Senior Leadership Team and the designated Safeguarding Governor to discuss current issues, review incident logs and filtering/change control logs • Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • Ensure that online safety incidents are logged as a safeguarding incident • Facilitate training and advice for all staff • Oversee any pupil surveys / pupil feedback on online safety issues • Liaise with the Local Authority and relevant agencies • Are regularly updated in online safety issues and legislation, and are aware of the potential for serious child protection concerns.

Role	**Key Responsibilities**
Governors (including Safeguarding and online safety)	• Ensure that the school has in place policies and practices to keep the children and staff safe online • Approve the Online Safety Policy and review the effectiveness of the policy • Support the school in encouraging parents and the wider community to become engaged in online safety activities
Computing Curriculum Leader	• Oversees the delivery of the online safety element of the Computing curriculum

Network Manager/technician	• Reports online safety related issues to the Designated Safeguarding Officers • Manages the school's computer systems, ensuring - school passwords are kept confidential - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices - the school's policy on web filtering is applied and updated on a regular basis • Keeps up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • Checks that school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher • Keeps up-to-date documentation of the school's online security and technical procedures
Data Protection Officer	• Responsibility for data protection compliance
Business Manager	• Ensures that the data they manage is accurate and up-to date. • Reports data related safety issues that come to their attention, to the Designated Safeguarding Officers and the Data Protection Officer • Ensures best practice in information management. I.e. has appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. • Ensures the school is registered with Information Commissioner

Role	**Key Responsibilities**
Teachers	• Embed online safety in the curriculum • Supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)

All staff, volunteers and contractors.	• Report any suspected misuse or problem to the data protection officer • Maintain an awareness of current online safety issues and guidance e.g. through CPD • Model safe, responsible and professional behaviours in their own use of technology. • At the end of the period of employment or volunteering return any equipment or devices loaned by the school. This includes leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
Pupils	• Understand the importance of reporting abuse, misuse or access to inappropriate materials • Know what action to take if they or someone they know feels worried or vulnerable when using online technology • 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 • Contribute to any 'pupil voice' / surveys that gathers information of their online experiences
Parents/carers	• Consult the school if they have any concerns about their children's use of technology • Support the school in promoting online safety.
External groups including Parent groups	• Any external individual/organisation must sign an Acceptable Use agreement prior to using technology or the Internet within school • Support the school in promoting online safety • Model safe, responsible and positive behaviours in their own use of technology.

1. Education and Curriculum

Pupil online safety curriculum

This school:

- Has a clear, progressive online safety education programme as part of the Computing curriculum. 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;
- Ensures pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

- Supports children and families to use key online platforms and tools safely and consistently throughout the school;
- 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;

Staff and Governor Training

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program;
- 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 Online Safety Policy and the school's Acceptable Use Agreements.

Parent awareness and training

The school provides guidance for parents and carers about online safety including informing parents about what activities their children are being asked to do online at school and the sites they will be asked to access. Teachers will inform parents if and when their children going to be interacting with anyone online as part of their learning.

On-line safety information in school

- On-line Safety is taught through the updated Teach Computing curriculum and through some PSHE lessons. The school holds annual E-safety events often in Online safety week or on Safer Internet Day.
- All staff are given a copy of the on-line -safety policy and its application and importance explained. The policy is made available for supply teachers. All staff are asked to sign an acceptable use policy. Training on e-safety is provided.

2. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences
- understand it is essential to immediately report abuse, misuse or access to inappropriate materials and know how to do so
- understand the importance of adopting good online safety practice when using digital technologies in and out of school

- know and understand school policies on the use of mobile and hand held devices including cameras
- store all personal data in lockable storage cabinets or a lockable storage area.

Staff and volunteers

- know to be vigilant in the supervision of children at all times, and have control over online learning resources when children are working on computers
- 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.

Parents/Carers

- as part of the School's admission form, parents support the school's on-line safety acceptable use agreement form.
- know and understand what the school's rules of appropriate use for the whole school community' are and what sanctions result from misuse.

Handling Incidents:

- the school will take all reasonable precautions to ensure online safety
- staff and pupils are given information about infringements in use and possible sanctions
- the Designated Safeguarding Officer acts as first point of contact for any incident along with the Data Protection Officer
- any suspected online risk or infringement is reported to the Designated Safeguarding Lead and the Data Protection Officer
- any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors, the LADO (Local Authority's Designated Officer) and the DPO (Data Protection Officer)
- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions
- all members of the school are encouraged to be vigilant in reporting issues, in the confidence they will be dealt with quickly and sensitively, through the school's escalation processes
- support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues
- monitoring and reporting of online safety incidents takes place and contributes to developments in policy and practice in online safety within the school
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible

- the Police will be contacted if one of our staff or pupils receives online communication that has serious safeguarding implications or breaks the law
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

3. Managing IT and Communication System

Internet access, security (virus protection) and filtering

This school:

- informs all users that Internet/email use could be monitored by the Head if an issue arises which requires investigation
- has filtered secure broadband connectivity through Schools TST and uses it to block inappropriate sites e.g. adult content, race hate, and gaming. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status
- uses DfE and LA approved systems including, secure file/email to send 'protect-level' (sensitive personal) data over the Internet
- does not allow staff to access 'protect-level' (sensitive personal) online data off-site
- works in partnership with the Schools TST to ensure any concerns about the system are communicated so that systems remain robust and protect students.

Network management (user access, backup)

- uses guest accounts occasionally for external or short-term visitors for temporary access to appropriate services
- uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful
- ensures the Systems Administrator/network manager is up-to-date with LA services and policies/requires the Technical Support Provider to be up-to-date with LA services and policies
- has daily back-up of school data (admin and curriculum)
- storage of all data within the school will conform to the EU and UK data protection requirements.

To ensure the network is used safely, the school:

- ensures staff read and sign that they have understood the school's online safety Policy. This applies to their 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.
- 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

- 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 log off when they have finished working or are leaving the computer unattended
- ensures all equipment owned by the school and/or connected to the network has up to date virus protection
- makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities
- makes clear that staff accessing LA systems do so in accordance with any Corporate policies
  e.g. County email or Intranet; finance system, Personnel system etc.
- maintains equipment to ensure Health and Safety is followed
- ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems
- does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems
- has a clear disaster recovery system in place that includes a secure, remote off site back up of data
- uses secure data transfer; this includes DfE and LA secure systems for all Common Transfer Files sent to other schools
- our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use
- all IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards
- we ask staff to undertake house-keeping checks at least annually to review, remove and destroy any digital materials and documents which no longer need to be stored.

Password policy

- This school makes it clear that staff must always keep their passwords private, must not share with others; if a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords.
- We require staff using critical systems to use two-factor authentication.

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

- use anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk/head@schoolname.la.sch.uk/or class e-mail addresses
- will contact the Police if one of our staff receives an e-mail that we consider is particularly disturbing or breaks the law
- ensures that email accounts are maintained and up to date
- uses LA-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses
- ensures pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home

Staff:

- staff will use LA e-mail systems for professional purposes
- never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained
- The school web site complies with statutory DFE requirements
- 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
- 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.

Social networking

Staff, Volunteers and Contractors:

- Staff are instructed to always keep professional and private communication separate.
- 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.
- The use of any school approved social networking will adhere to the staff protocol, code of conduct and data protection legislation.

School staff will ensure that in private use:

- no reference should be made in social media to pupils, parents/carers or school staff
- school staff should not be on-line friends with any pupil
- 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
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- are required to sign and follow our age appropriate pupil Acceptable Use Agreement.

Parents:

- are reminded about social networking risks and protocols
- are reminded that they need to ask permission before uploading photographs, videos or any other information about other people
- are advised not to comment on other children or parents on their own social network sites.

4. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- the Headteacher is the Senior Information Risk Officer (SIRO)
- staff are clear who the key contact are for key school information are. We have listed the information and information asset owners
- 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 a single central record

Technical Solutions

- staff have secure area(s) on the network to store sensitive documents or photographs
- we require staff to lock their desktop when leaving their computer.
- paper based sensitive information is either shredded using a cross-cut shredder or collected and stored in a lockable storage area to be bulk shredded by a company who complies with the GDPR and provides a certificate of destruction
- we use encrypted flash drives if any member of staff has to take any sensitive information off site
- we use the DfE S2S site to securely transfer CTF pupil data files to DfE/other schools
- 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
- 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.

Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data

5. Equipment and Digital Content

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

- 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 devices.
- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, or their families within or outside school. Personal phones cannot be used during lessons or formal school time. However, staff may use their own phone to contact the school when off-site with pupils i.e. when on a class trip.
- Staff members may use their phones during school break times away from areas occupied by children.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- All visitors are requested to keep their phones on silent.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.
- Staff, visitors and volunteers 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.

Digital images and video

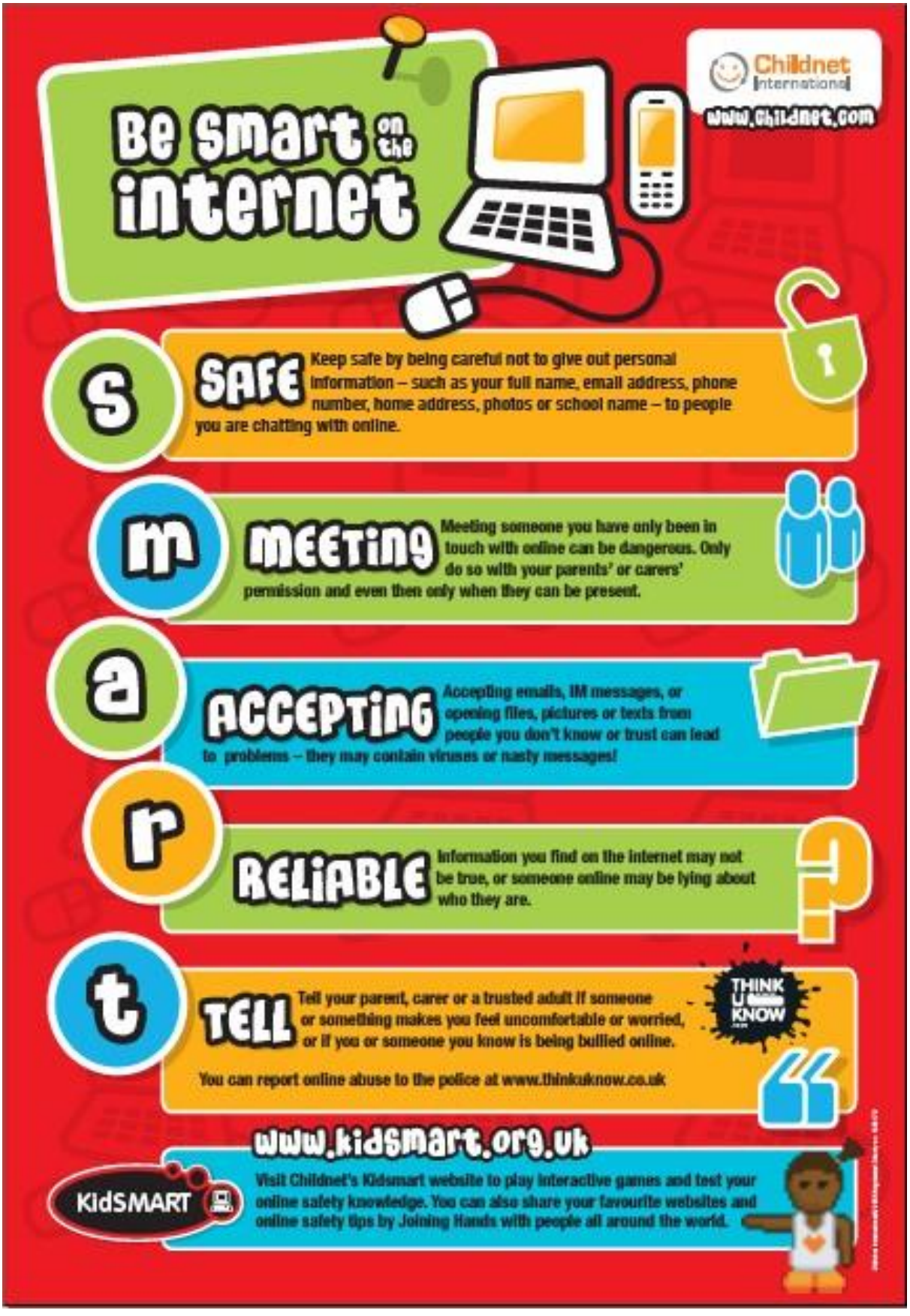
In this school:

- we gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their 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/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, high profile use
- we block/filter access to social networking sites unless there is a specific approved educational purpose

- pupils are taught about how images can be manipulated in their online 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

APPENDICES

A1 SMART Poster



A2 EYFS & KS1 Acceptable Use Policy

Haddenham St Mary's CE School

EYFS & KS1 Acceptable Use Policy

Think before you click!!

Are you being?

I will only use the internet and email with an adult.

Click on icons and links when I know they are safe or when my teacher has asked me to.

I will only send friendly and polite messages and will only send them to people I know and trust.

Every time

I see something I don't like on screen, I will always tell an adult straight away.

A3: Additional information and guidance

More information can be found KCSiE2025

DfE advice for schools: teaching online safety in schools

UK Council for Online safety (UKCIS) 37 guidance: Education for a connected world

UKCIS guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people.

The UKCIS external visitor's guidance will help schools and colleges to ensure the maximum impact of any online safety sessions delivered by external visitors

National Crime Agency's CEOP education programme: Thinkuknow

Public Health England38: Every Mind Matters