Harlowbury "Believe, Succeed, Inspire"
Primary School

On-line Safety Policy
Autumn 2017

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school's community with respect to the use of IT-based technologies.
- Safeguard and protect all of our children and staff.
- Assist staff working with children 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 and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school's community.
- Have clear structures to deal with online abuse such as online bullying or harassment.
- Ensure that all members of the 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
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

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

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

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

Role	Key Responsibilities
Head teacher DSL	Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance; • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school's safeguarding. • To take overall responsibility for online safety provision; • To take overall responsibility for data management and information security (SIRO) ensuring schools' relevant Local Safeguarding Children Board (LSCB) guidance • To ensure the school uses appropriate IT systems and services including, filtered Internet Service; • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles; • To be aware of procedures to be followed in the event of a serious online safety incident; • Ensure suitable 'risk assessments' undertaken so the curriculum meets the needs of students, including risk of children being radicalised; • To receive regular monitoring reports from the Online Safety Co-coordinator; • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, • To ensure Governors are regularly updated on the nature and effectiveness of the schools' arrangements for online safety; • To ensure the school website includes relevant information.
DSL Deputy Head Teacher	Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the schools' safety policy/documents • Promote an awareness and commitment to online safety throughout the school's community; • Ensure that online safety education is embedded within the curriculum; • Liaise with school's technical staff where appropriate; • To communicate regularly with SLT and the designated online safety governor/committee to discuss current issues, review incident logs and filtering/change control logs; • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident; • To ensure that online safety incidents are logged as a safeguarding incident; • Facilitate training and advice for all staff; • Oversee any student surveys / feedback on online safety issues;

Role	Key Responsibilities
	• Liaise with the Local Authority and relevant agencies; • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
Governors/Safeguarding governor (including online safety)	• To ensure that the school has in place policies and practices to keep the children and staff safe online; • To approve the Online Safety Policy and review the effectiveness of the policy; • To support the school in encouraging parents and the wider community to become engaged in online safety activities; • The role of the online safety Governor will include: regular review with the online safety coordinator.
Computing Leader	• To oversee the delivery of the online safety element of the Computing curriculum. • To ensure the curriculum, technologies and devices used in school support raising standards of achievement for all pupils.
Network Manager/Technician	To report online safety related issues that come to their attention, to the Online Safety Coordinator; • To manage the school network and make sure that: -school password policy is strictly adhered to and reset termly for all users - 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. • That they keep 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; • That the use of school technology and online platforms are regularly monitored and that any misuse/attempted is reported to the online safety leader /head teacher • To ensure appropriate backup procedures and disaster recovery plans are in place; • To keep up-to-date documentation of the school disaster recovery plans
Data and Information Manager/Office Staff	• 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;
Teachers	• To embed online safety in the curriculum; • To supervise and guide students carefully when engaged in learning activities involving online technology (including, extra-curricular and extended activities if relevant); • To ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff, Volunteers and visitors.	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by new staff on induction; • To report any suspected misuse or problem to the online safety coordinator; • To maintain an awareness of current online safety issues and guidance e.g. through CPD;

Role	Key Responsibilities
	• To model safe, responsible and professional behaviours in their own use of technology. • At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include 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	• Read, understand, sign and adhere to the Student Acceptable Use Policy annually; • 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 the school • To have the opportunity to become Digital Leaders.
Parents and Carers	• To read, understand and promote the school's Student Acceptable Use Agreement with their child/children; • To consult with the school if they have any concerns about their children's use of technology; • To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the students' use of the Internet and the school's use of photographic and video images.

Communication

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

- Policy to be published on the school website/ staffroom/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 Incidents

The school will take all reasonable precautions to ensure online safety.

• Staff and students are given information about infringements in use and possible sanctions.

• Online Safety Leader acts as first point of contact for any incident.

• Any suspected online risk or infringement is reported to Online Safety Leader that day.

• Any concern about staff misuse is always referred directly to the Head, unless the concern is about the Head in which case the compliant is referred to the Chair of Governors.

Education and Curriculum

Why is Internet use important?

● The Internet is a part of everyday life for education, business and social interaction.
● The school has a duty to provide children with quality Internet access as part of their learning experience.
● Children use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
● The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
● Internet access is an entitlement for children who show a responsible and mature approach to its use.

Harlowbury Primary School:-

• Has a clear, online safety education programme as part of the Computing curriculum/PSHE/P4C curriculum and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to the children's 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 through the student Acceptable Use Agreement(s);

Ensure children learn to manage their own risks within use of the internet, technologies and the "virtual" world.

• 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, and use of content, research skills, copyright;

• Ensures that staff and students understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;

• Ensure students only use school approved systems and publish within appropriately secure and age-appropriate environments.

Staff and governor training

Harlowbury School:-

- Makes regular training available to staff and governors 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 work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

Parent awareness

The school:

- Takes every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / information about national / local online safety campaigns / literature.
- Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of such as not taking photographs or videos during school events.

3. Expected Conduct and Incident Management

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 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 the school;
- Know and understand school policies on the use of mobile and hand held devices including cameras.

Staff, volunteers and contractors

• 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 students have more flexible access;

• Know to take professional, reasonable precautions when working with students, previewing websites before use; using age-appropriate (student friendly) search engines where more open Internet searching is required with younger students;.

Parents/Carers

• Should provide consent for students to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;

• Should know and understand what the school's rules of appropriate use for the whole school community are and what sanctions result from misuse.

Incident Management

In this school:

• There is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;

• All members of the school and community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively

• Support is actively sought from other agencies as needed (e.g. UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, MASH) in dealing with online safety issues;

• 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 students receives online communication that we consider is particularly disturbing or breaks the law;

• Immediate referrals to the police or MASH will be made if online materials/communications show:-

- an adult is involved
- coercion/blackmail is involved,
- extreme or violent behaviours,
- the child is under the age of 13
- is at the immediate risk of harm

4. Managing Information Systems

- **Internet access, security (virus protection) and filtering**

This school:

- Has the educational filtered secure broadband connectivity through the Essex County Council.
- Uses the Essex County Council Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, the Police or CEOP;
- The school access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers;
- Changes to the filtering policies are updated by the ICT Technician as directed by the Senior Leadership Team;
- Ensure network health through use of suitable anti-virus software;
- Use DfE approved systems including DfE S2S, to send 'protect-level' sensitive / personal data over the Internet;
- Use encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site.

- **Network management (user access, backup)**

  This school

  - Uses individual log-ins for all users.
  - 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 ECC services and policies / requires the Technical Support Provider to be up-to-date with ECC services and policies.
  - Stores all of its 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 username and password.
- Staff access to the schools' management information system is controlled through a separate password for data security purposes.
- 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, the Learning Platform and (for older pupils) their own school approved email account when supplied.
- 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.
- 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 and we also automatically switch off all computers to save energy.
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes.
- Scans all mobile equipment with anti-virus software protection.
- 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.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies.
  e.g. Borough email or Intranet; finance system, Personnel system etc.
- 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 / LA electrical engineers.

- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems:
  e.g. teachers access their area / a staff shared area for planning.
- 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.
  e.g. technical support or RM INTEGRIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child.
- Provides pupils and staff with access to content and resources through the approved Learning Platform (when supplied) which staff and pupils access using their username and password.
- Makes clear responsibilities for the daily back up of RM INTEGRIS and finance systems and other 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.
- Uses the DfE secure s2s (or similar) website for all CTF files sent to other schools.
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA.
- 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 RM INTEGRIS system.
- We require staff to regularly change their passwords into the RM INTEGRIS 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.
- Provides highly restricted (Safe mail) / simulated environments for e-mail with Key Stage 1 pupils.

- 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@schoolname.la.sch.uk / head@schoolname.la.sch.uk / or class e-mail addresses (with one or more staff having access to an aliased/shared mailbox for a class) 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 e-mail 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.

Pupils:

- Pupils are introduced to, and use e-mail as part of the ICT/Computing scheme of work.

- 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 only use the school e-mail systems for professional purposes.
- Access in school to external personal e mail accounts may be blocked.
- Never use e-mail to transfer staff or pupil personal data. We use secure, LA / DfE approved systems.
- 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.
- 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 LA / School Agreement Form to say they have read and understood the On Line 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.
- 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. info@schooladdress or admin@schooladdress. 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.

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.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

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 (the Information Asset Owners) are.
- 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.
- 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 follow LA guidelines for the transfer of any 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. 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, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertake 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 area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer
- 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 other schools.
- We use S2S to transfer other data to schools , such as references, reports of children.
- 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 ECC off site backup for disaster recovery on our admin network.
- 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.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, pupils & parents or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Pupil mobile phones which are brought into school must be given to the office. Staff members may use their phones during school break times.
  All visitors are requested to keep their phones on silent.

- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. 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 pupils 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 seek specific premises to use their phone at other than their break times.
- 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.

Pupils' use of personal devices

- The School strongly advises that student mobile 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 and children will drop their phones off in the office in the morning and collect at the end of the day.
- 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.
- If a pupil 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.
- 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 within or outside of the setting in a professional capacity.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or 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.
- 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, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

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.
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils.
- 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 ICT scheme of work.
- Pupils are advised not to place any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission . We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

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.

7. Appendices

- Appendix 1 - Acceptable User Policies
- Appendix 2 On Line Safety Record Form
- Appendix 3 - Online Safety Resources

Appendix Children's Acceptable Use Policy

Harlowbury Primary School

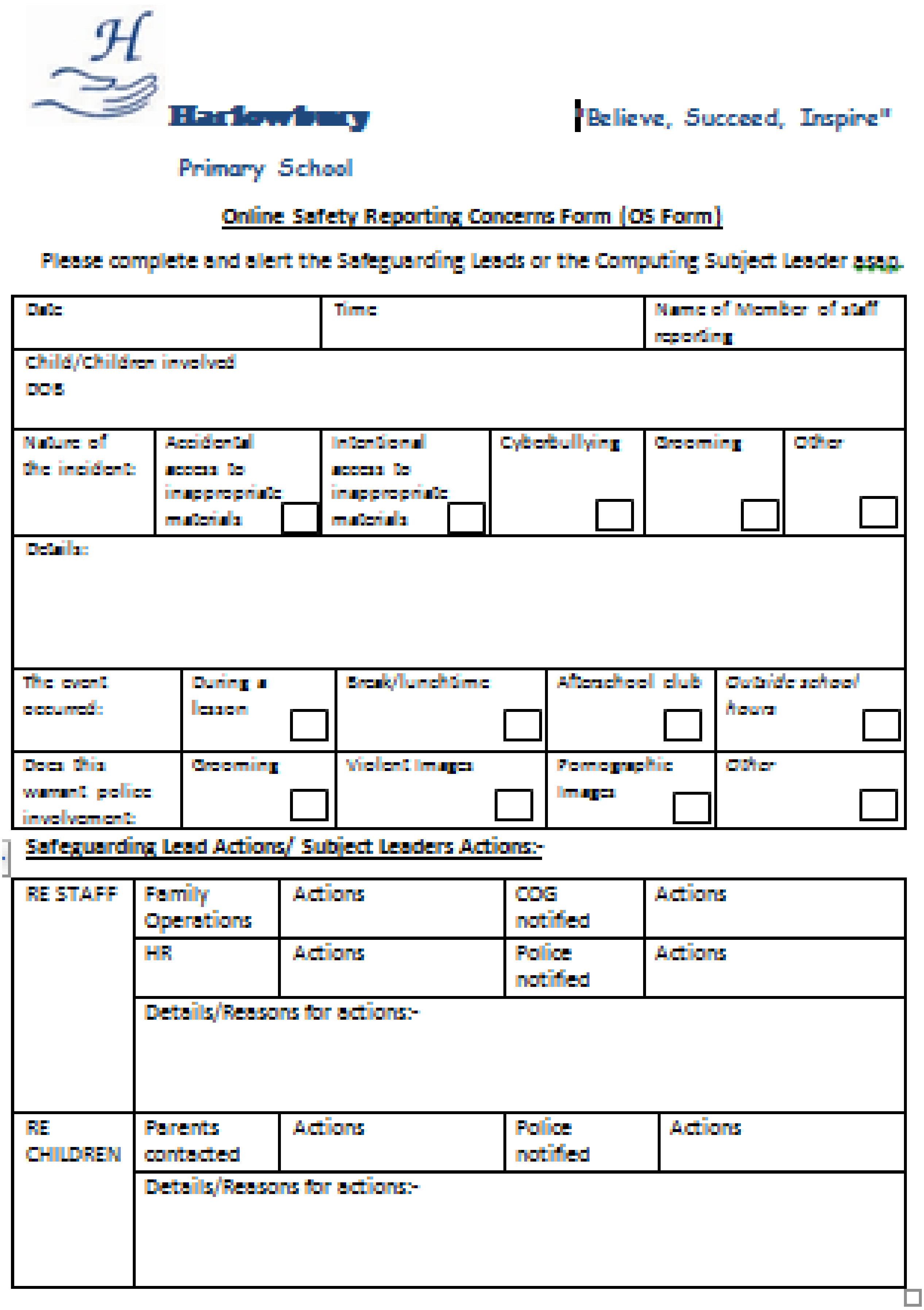
Responsible Use of the Internet

- I will not arrange to meet anyone contacted over the Internet.
- I will not try to find unacceptable material from the Internet.
- I will not give my full name, home address or telephone number to anyone over the Internet.
- I will only use the Internet when I have permission and/or am supervised by a teacher.
- I will only email people my teacher has approved.
- I will respect the privacy of others. I will not publish their names, addresses, phone numbers or photographs.
- I will use the Internet only for activities and work set by school e.g. homework, topic work.
- I will report any unpleasant material or messages sent to me. I understand that this will help to protect other pupils and myself.
- I will not sent unsuitable email messages, my messages will be polite, responsible and only signed in my name.
- I know that the school may check my computer files and may monitor the Internet sites I visit.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

<table>
<tr><td colspan="2"><b>Harlowbury School</b>
<b>Responsible Use of the Internet and Social Media</b></td></tr>
<tr><td><b>Pupil:</b></td><td><b>Class:</b></td></tr>
<tr><td colspan="2"><b>Pupil's Agreement</b>
I have read and understand the school Rules for Responsible Use of the Internet and Social Media. I will use the Internet in a responsible way and follow these rules at all times. In particular, I will not share my password with anybody else. I will not give out my name, home address, photographs or phone number in messages or write messages that I would not let my teachers and parents read. If I receive an e-mail, text or message which upsets me or is from somebody I don’t know, I will tell my teacher immediately.</td></tr>
<tr><td><b>Signed:</b></td><td><b>Date:</b></td></tr>
<tr><td colspan="2"><b>Parent's/ Carer’s Consent for Internet and Social Media.</b>
I have read and understood the school rules for responsible use of the Internet and Social Media and give permission for my son / daughter to access this. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet.
I will ensure that my child understands the importance of keeping their password private and have discussions with them about how to stay safe whilst using the Internet, online gaming consoles and social media.</td></tr>
<tr><td><b>Signed:</b></td><td><b>Date:</b></td></tr>
</table>

Appendix Online Safety School Record



Harlowbury Primary School

"Believe, Succeed, Inspire"

Online Safety Reporting Concerns Form (OS Form)

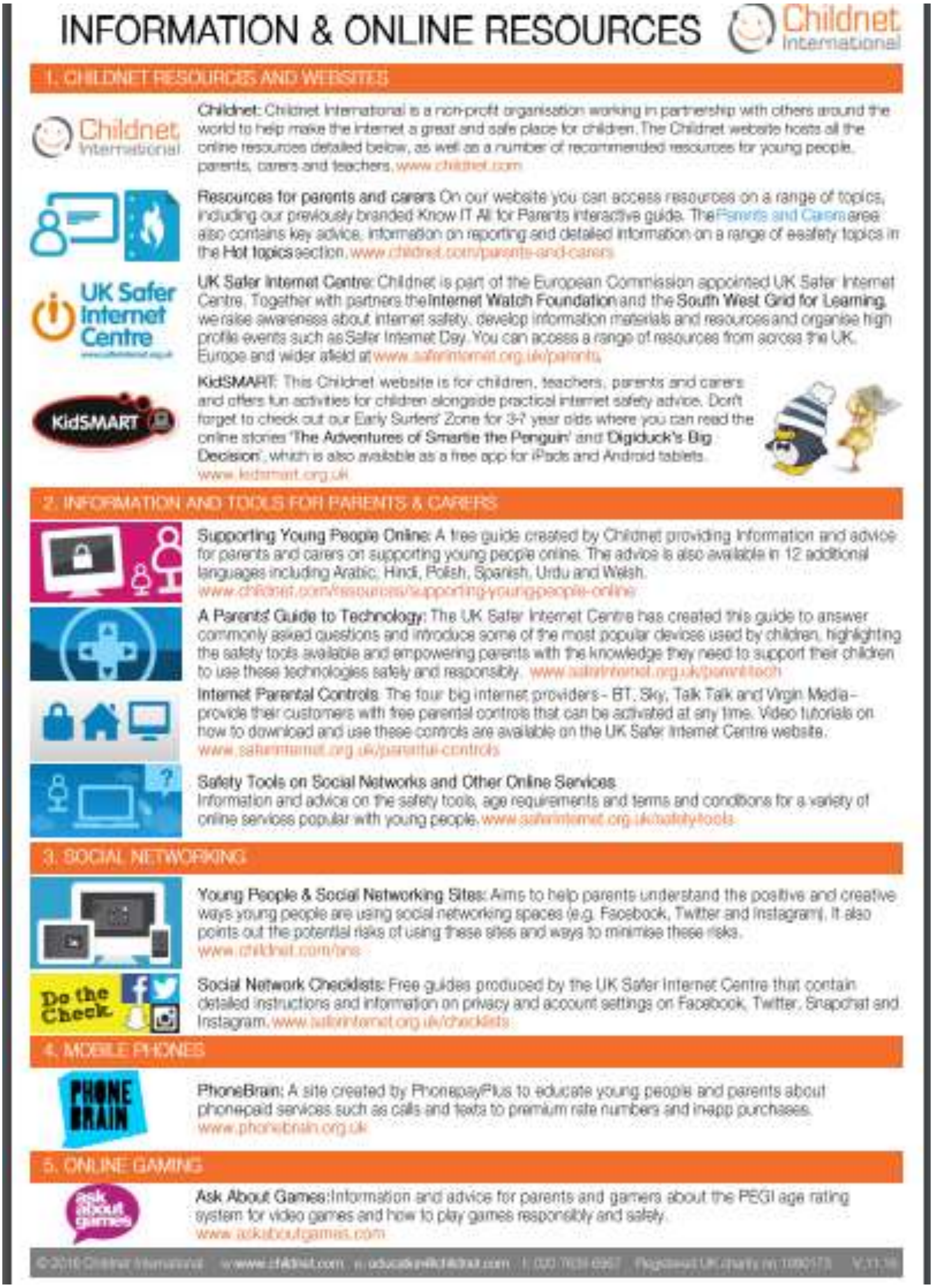
Please complete and alert the Safeguarding Leads or the Computing Subject Leader asap.

Date	Time		Name of Member of staff reporting		
Child/Children involved DOB					
Nature of the incident:	Accidental access to inappropriate materials □	Intentional access to inappropriate materials □	Cyberbullying □	Grooming □	Other □
Details:					
The event occurred:	During a lesson □	Break/lunchtime □	Afterschool club □	Outside school/ hours □	
Does this warrant police involvement:	Grooming □	Violent images □	Pornographic images □	Other □	

Safeguarding Lead Actions/ Subject Leaders Actions:-

RE STAFF	Family Operations	Actions	COG notified	Actions
	HR	Actions	Police notified	Actions
	Details/Reasons for actions:-			
RE CHILDREN	Parents contacted	Actions	Police notified	Actions
	Details/Reasons for actions:-			

Appendix Online Safety Resources



INFORMATION & ONLINE RESOURCES

Childnet International

1. CHILDNET RESOURCES AND WEBSITES

Childnet: Childnet International is a non-profit organisation working in partnership with others around the world to help make the internet a great and safe place for children. The Childnet website hosts all the online resources detailed below, as well as a number of recommended resources for young people, parents, carers and teachers. www.childnet.com

Resources for parents and carers On our website you can access resources on a range of topics, including our previously branded Know IT All for Parents interactive guide. The Parents and Carers area also contains key advice, information on reporting and detailed information on a range of esafety topics in the **Hot topics** section. www.childnet.com/parents-and-carers

UK Safer Internet Centre: Childnet is part of the European Commission appointed UK Safer Internet Centre. Together with partners the **Internet Watch Foundation** and the **South West Grid for Learning**, we raise awareness about internet safety, develop information materials and resources and organise high profile events such as Safer Internet Day. You can access a range of resources from across the UK, Europe and wider afield at www.saferinternet.org.uk/parents.

KidSMART: This Childnet website is for children, teachers, parents and carers and offers fun activities for children alongside practical internet safety advice. Don't forget to check out our Early Surfers' Zone for 3-7 year olds where you can read the online stories '**The Adventures of Smartie the Penguin**' and '**Digiduck's Big Decision**', which is also available as a free app for iPads and Android tablets. www.kidsmart.org.uk

2. INFORMATION AND TOOLS FOR PARENTS & CARERS

Supporting Young People Online: A free guide created by Childnet providing information and advice for parents and carers on supporting young people online. The advice is also available in 12 additional languages including Arabic, Hindi, Polish, Spanish, Urdu and Welsh. www.childnet.com/resources/supporting-young-people-online

A Parents' Guide to Technology: The UK Safer Internet Centre has created this guide to answer commonly asked questions and introduce some of the most popular devices used by children, highlighting the safety tools available and empowering parents with the knowledge they need to support their children to use these technologies safely and responsibly. www.saferinternet.org.uk/parent-tech

Internet Parental Controls: The four big internet providers - BT, Sky, Talk Talk and Virgin Media - provide their customers with free parental controls that can be activated at any time. Video tutorials on how to download and use these controls are available on the UK Safer Internet Centre website. www.saferinternet.org.uk/parental-controls

Safety Tools on Social Networks and Other Online Services
Information and advice on the safety tools, age requirements and terms and conditions for a variety of online services popular with young people. www.saferinternet.org.uk/safety-tools

3. SOCIAL NETWORKING

Young People & Social Networking Sites: Aims to help parents understand the positive and creative ways young people are using social networking spaces (e.g. Facebook, Twitter and Instagram). It also points out the potential risks of using these sites and ways to minimise these risks. www.childnet.com/sns

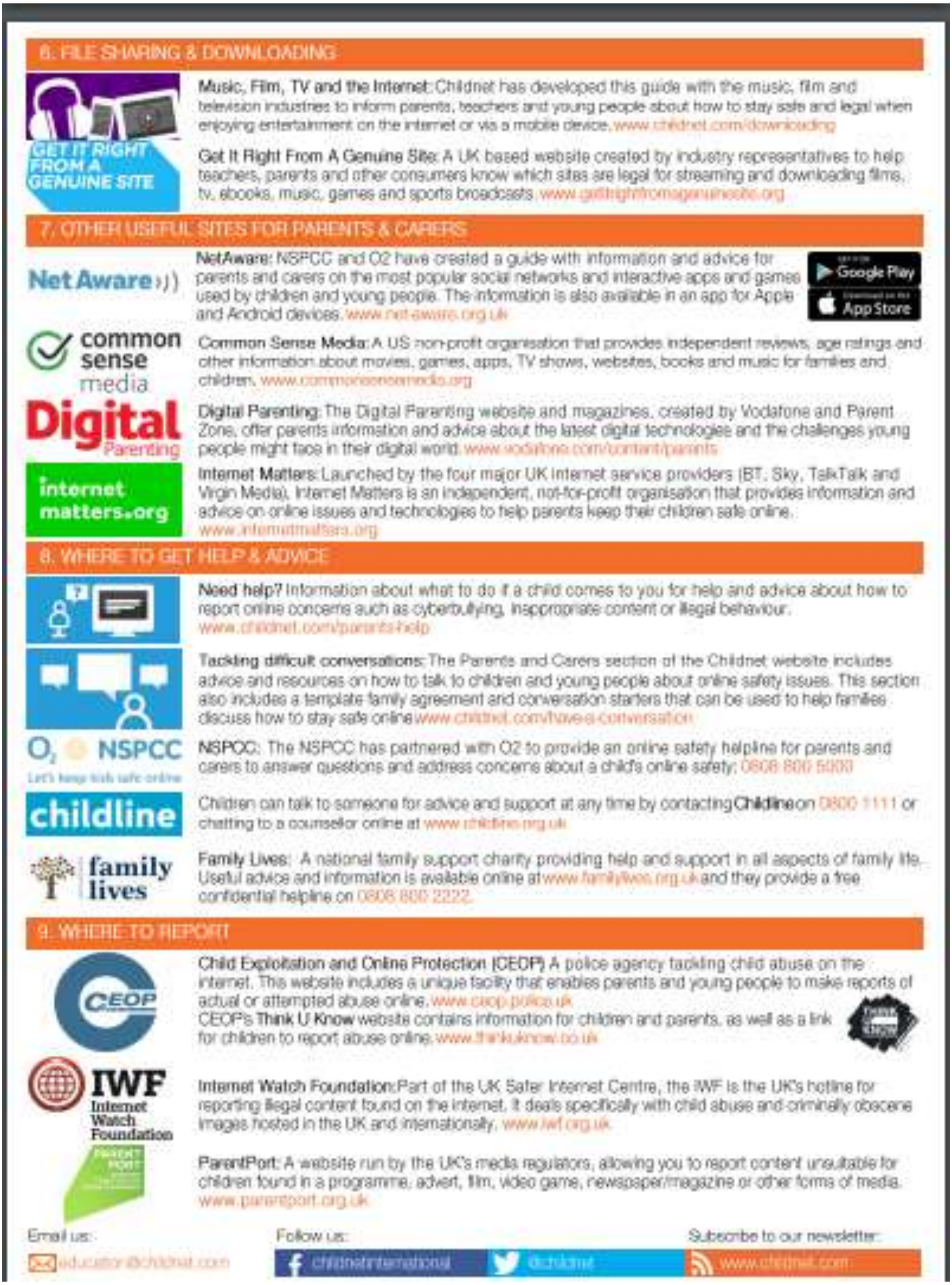
Social Network Checklists: Free guides produced by the UK Safer Internet Centre that contain detailed instructions and information on privacy and account settings on Facebook, Twitter, Snapchat and Instagram. www.saferinternet.org.uk/checklists

4. MOBILE PHONES

PhoneBrain: A site created by PhonepayPlus to educate young people and parents about phonepaid services such as calls and texts to premium rate numbers and inapp purchases. www.phonebrain.org.uk

5. ONLINE GAMING

Ask About Games: Information and advice for parents and gamers about the PEGI age rating system for video games and how to play games responsibly and safely. www.askaboutgames.com



6. FILE SHARING & DOWNLOADING

Music, Film, TV and the Internet: Childnet has developed this guide with the music, film and television industries to inform parents, teachers and young people about how to stay safe and legal when enjoying entertainment on the internet or via a mobile device. www.childnet.com/downloading

Get It Right From A Genuine Site: A UK based website created by industry representatives to help teachers, parents and other consumers know which sites are legal for streaming and downloading films, tv, ebooks, music, games and sports broadcasts. www.getitrightfromagenuinesite.org

7. OTHER USEFUL SITES FOR PARENTS & CARERS

NetAware: NSPCC and O2 have created a guide with information and advice for parents and carers on the most popular social networks and interactive apps and games used by children and young people. The information is also available in an app for Apple and Android devices. www.net-aware.org.uk

Common Sense Media: A US non-profit organisation that provides independent reviews, age ratings and other information about movies, games, apps, TV shows, websites, books and music for families and children. www.commonsensemedia.org

Digital Parenting: The Digital Parenting website and magazines, created by Vodafone and Parent Zone, offer parents information and advice about the latest digital technologies and the challenges young people might face in their digital world. www.vodafone.com/content/parents

Internet Matters: Launched by the four major UK internet service providers (BT, Sky, TalkTalk and Virgin Media), Internet Matters is an independent, not-for-profit organisation that provides information and advice on online issues and technologies to help parents keep their children safe online. www.internetmatters.org

8. WHERE TO GET HELP & ADVICE

Need help? Information about what to do if a child comes to you for help and advice about how to report online concerns such as cyberbullying, inappropriate content or illegal behaviour. www.childnet.com/parents-help

Tackling difficult conversations: The Parents and Carers section of the Childnet website includes advice and resources on how to talk to children and young people about online safety issues. This section also includes a template family agreement and conversation starters that can be used to help families discuss how to stay safe online www.childnet.com/have-a-conversation

NSPCC: The NSPCC has partnered with O2 to provide an online safety helpline for parents and carers to answer questions and address concerns about a child's online safety: 0808 800 5002

Children can talk to someone for advice and support at any time by contacting **Childline** on 0800 1111 or chatting to a counsellor online at www.childline.org.uk

Family Lives: A national family support charity providing help and support in all aspects of family life. Useful advice and information is available online at www.familylives.org.uk and they provide a free confidential helpline on 0808 800 2222.

9. WHERE TO REPORT

Child Exploitation and Online Protection (CEOP) A police agency tackling child abuse on the internet. This website includes a unique facility that enables parents and young people to make reports of actual or attempted abuse online. www.ceop.police.uk
CEOP's **Think U Know** website contains information for children and parents, as well as a link for children to report abuse online. www.thinkuknow.co.uk

Internet Watch Foundation: Part of the UK Safer Internet Centre, the IWF is the UK's hotline for reporting illegal content found on the internet. It deals specifically with child abuse and criminally obscene images hosted in the UK and internationally. www.iwf.org.uk

ParentPort: A website run by the UK's media regulators, allowing you to report content unsuitable for children found in a programme, advert, film, video game, newspaper/magazine or other forms of media. www.parentport.org.uk

Email us: education@childnet.com

Follow us: childnetinternational @childnet

Subscribe to our newsletter: www.childnet.com

This policy will be reviewed in Spring 2018 in line with the new requirements for General Data Protection Regulation which comes into regulation May 2018.