ORLEY FARM
SCHOOL

# E-Safety Policy

(Whole School Including EYFS)

| | | | |
|---|---|---|---|
| **First Issued:** | February 2011 | **Next Review:** | Spring Term 2027 |
| **Last Reviewed:** | Spring Term 2025 | **Version:** | 4.3 |
| **Responsible:** | Deputy Head Pastoral (and DSL) | | |

## Safeguarding Statement

At Orley Farm School, we respect and value all children and are committed to providing a safe, caring, friendly environment in which our pupils can learn securely. We believe every pupil should be able to participate in all school activities in a safe, harm free, enjoyable environment. This is the responsibility of every adult employed by or invited to deliver services at Orley Farm School. It is our responsibility to safeguard all who access school and to promote the welfare of all our pupils by protecting them from physical, sexual and emotional abuse, neglect and bullying.

### 1. Aims

To support Orley Farm School's Safeguarding and Curriculum Policies, by defining the school's approach to E-Safety. This recommends best practice on how to support pupils whilst using electronic devices and the Worldwide Web in school and at home. It recommends how staff can protect their own safety and security. It also aims to educate parents and make them aware of the risks children face at home.

### 2. Objectives

To ensure pupils and staff are aware of the issues surrounding E-Safety. This encompasses internet technologies, social networking and electronic communications.

### 3. World Wide Web

**a) The school will use firewalls to limit access to unsuitable material for all users. It will use software to monitor the usage of all devices in school and school devices used elsewhere.**

**b) Pupils' use of the World Wide Web in school is only permitted when supervised by an adult.**

c) If staff or pupils discover unsuitable sites, the URL (address), time and content must be reported to the Network Manager. Pupils can only use approved email accounts on the school system. These accounts are monitored by appropriate software.

d) Pupils are taught and encouraged to tell a trusted adult immediately if they receive offensive emails (either within school or at home) or should people unknown to them try to make contact.

e) Pupils are taught never to give out personal details of any kind, including their email address, in a public setting (virtual or real) or divulge personal details which might identify them or their location.

f) Use of social networking sites, newsgroups, forums and chat rooms in school is not permitted. Pupils can use educationally based websites that permit file sharing and pupil interaction. These websites are monitored and used subject to adult supervision.

g) Pupils are advised to never place personal photos on any website or post photos of others on websites or in messages without the explicit permission of those in the photos.

### 4. Devices

a. Pupils are not permitted to bring mobile phones onto the school site. Year 7 and Year 8 pupils can request permission to carry a phone should they be travelling to or from school independently. The request should be made in writing by parents/carers to the Deputy Head. In exceptional circumstances Year 6 pupils can also make this request. In these instances, phones should be switched off whilst on the school site or whilst off site and the pupil is engaged in a school/afterschool activity. During the school day phones should be left at the school office.

b. All users should understand that the use of personal devices in a school context is only for educational purposes. Teaching about the safe and appropriate use of mobile technologies is integral to the school's online safety education programme

**c. Mobile Phones in EYFS**

Any mobile phone carried into an EYFS location by parents and visitors, or whilst working with EYFS children, must be turned off and stored in a secure location.

## 5. Publishing Content and the School Website

a. On the school website the only contact details published are the school address, email and telephone number. Staff and pupils’ personal contact information is not published.

b. On pupils’ admission parents/carers are requested to complete the parental consent form relating to the publication of images or work of their child on Orley Farm School media platforms. The school maintains a current record of all parental preferences. This record must be checked before images/work are published. Parents are reminded that they can change their consent at any time.

c. Photographs that include pupils are selected carefully, subject to parental consent and are appropriate for the context.

d. Pupils' full names are never used on any media platform in association with photographs.

## 6. Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible indirectly for their employees’ acts during their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability, or defame a third party might render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise the risk of harm to pupils, staff and the school:

a. Ensuring that personal information is not published.
b. Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
c. Clear reporting guidance, including responsibilities, procedures and sanctions.
d. Risk assessment, including legal risk.
e. They do not engage in online discussions on personal matters relating to members of the school community.
f. Personal opinions should not be attributed to the school.

When official school social media accounts are established, they must:

a. be approved by the marketing team and Head.
b. Have named users
c. A code of behaviour for named users of the accounts, including:
   i. Systems for reporting and dealing with abuse and misuse.
   ii. Understanding of how incidents may be dealt with under school disciplinary procedures.

### Personal Use

a. Personal communications are those made via personal social media accounts. In all cases, where a personal account is used that associates itself with the school or impacts the school it must be made clear that the staff member is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
b. Personal communications which do not refer to or impact the school are outside the scope of this policy.

c. Where excessive personal use of social media in school is suspected and considered to be interfering with relevant duties, disciplinary action may be taken. See Appendix 2 for code of conduct

d. The school permits reasonable and appropriate access to private social media sites.

**e.** Use of Digital/Video Images – see Staff Handbook.

## 7. Information System Security

a. Virus protection has been installed and is updated regularly by the Network Manager through anti-virus software.

b. Security strategies are discussed by the Senior Leadership Team, Network Manager and other relevant staff (E-Safety Group). The Network Manager then updates and implements changes to the system.

c. The school's wireless network is encrypted to prevent unauthorised access.

## 8. Education – Pupils

Whilst regulation and technical solutions are critical, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is essential to the school’s online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all curriculum areas, and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

a. A planned online safety curriculum should be provided as part of computing and PSHE Jigsaw lessons and should be regularly revisited *(Jigsaw curriculum Reception to Year 8 – please see Appendix - the E-Safety progression of skills document).*

b. Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities *(Safer-Internet Day & Student Voice assemblies).*

c. Pupils are taught, in all lessons involving IT equipment, to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.

d. Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

e. Pupils are taught that they are not allowed to use AI (unless instructed to do so by a teacher) to complete work set.

f. Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how to influence and participate in decision-making (PSHE Jigsaw curriculum).

g. Pupils are helped to understand the need for the ‘Pupil Acceptable Use Agreement’ and encouraged to adopt safe and responsible use both within and outside school.

h. Staff should act as good role models in their use of digital technologies, the internet and mobile devices.

i. In lessons, where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material found in internet searches.

j. Where pupils can search the internet freely, staff should be vigilant in monitoring the content of the websites the young people visit.

It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request the Network Manager to temporarily remove specific sites from the filtered list for the specific period of study. Any request to do so, should name the sites, reason for the request, dates and supervising staff. This information should be retained on an auditable Request Log.

## 9. Education – Parents/Carers

The school will seek to provide information and awareness to parents and carers through:

a. Learning Platform, 'Tooled Up'
b. Parents/carers coffee mornings
c. High-profile events/campaigns, e.g., Safer Internet Day

## 10. Assessing Risk

Every effort is taken to block inappropriate content in all situations however, there is no fail-safe way and therefore the school cannot take responsibility for these events when all reasonable steps have been taken.

## 11. Handling E-Safety complaints

a. Complaints of internet misuse at school or within school remit are dealt with by the Network Manager and a Deputy Head (Pastoral).

b. Any complaint about staff misuse must be referred to the Headmaster.

~~c.~~ Complaints of a child protection nature must be dealt with in accordance with the school child protection procedures - see the school's Safeguarding and Child Protection Policy.

## 12. Monitoring and Evaluation

The members of the Curriculum Team together with the E-Safety Group and Headmaster monitor and evaluate this policy.

### Schedule for Development/Monitoring/Review

| | |
|---|---|
| This online safety policy was approved by the Board of Governors on: | |
| The implementation of this online safety policy will be monitored by the following: | The Deputy Head of Pastoral (& DSL) and E-Safety Group |
| Monitoring will take place at regular intervals: | Annually |
| The Governing Body will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals: | Termly |
| The online safety policy will be reviewed annually or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be: | Summer term 2025 |
| Should serious online safety incidents take place, the following external persons/agencies should be informed: | LADO, Police. |

The school will monitor the impact of the policy using the following:

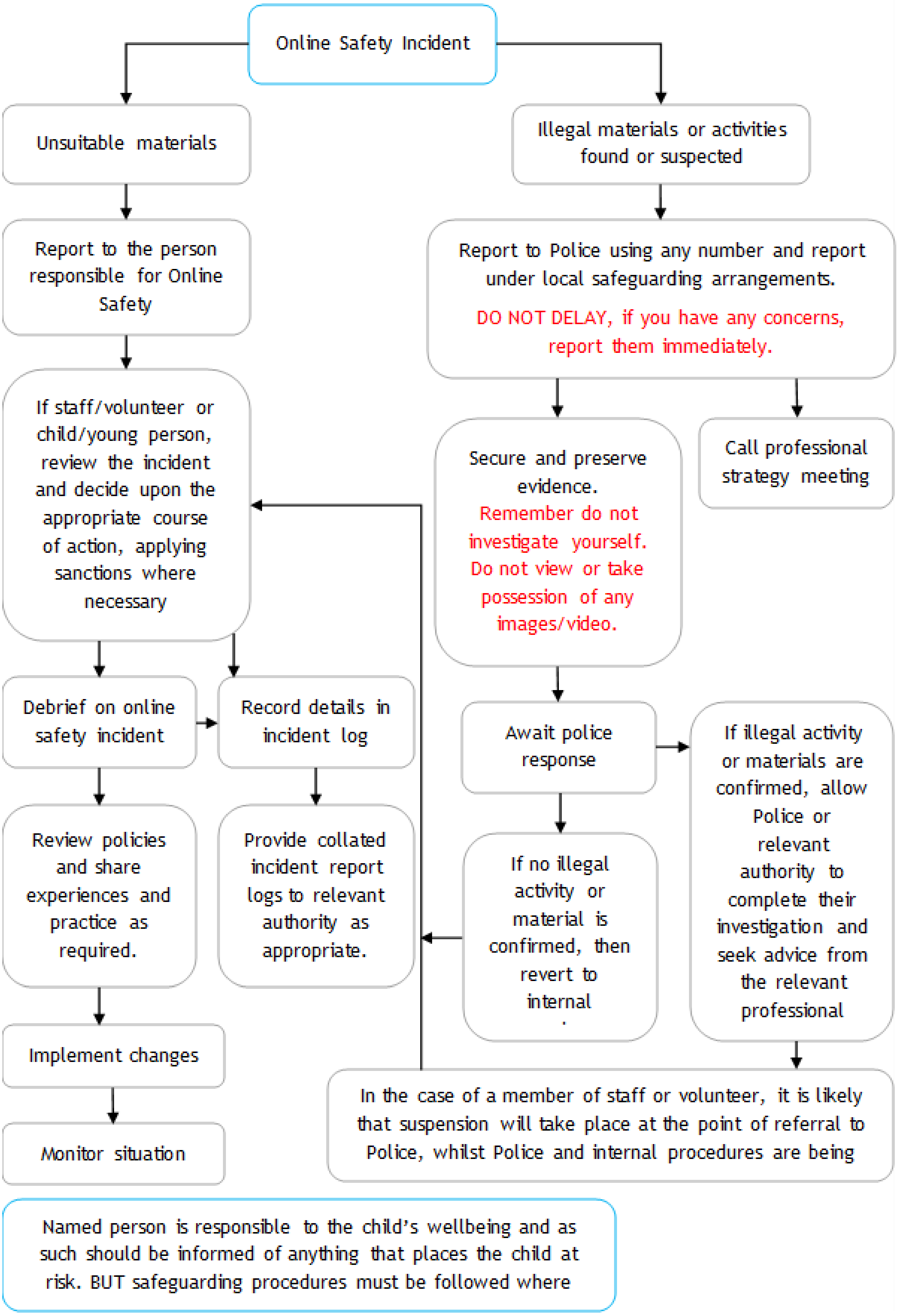
a. Logs of reported incidents
b. Monitoring logs of internet activity (including sites visited)/filtering)
c. Internal monitoring data for network activity

## 13. Responding to Incidents of Misuse

The flow diagram below is intended to assist management of incidents proportionately involving online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

### a. Illegal Incidents

If there is any suspicion that the incident concerned contains child abuse images, or any other suspected illegal activity, refer to the right-hand side of the flowchart and report immediately to the police.



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review policies and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate.

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/video.

Call professional strategy meeting

Await police response

If no illegal activity or material is confirmed, then revert to internal .

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional

In the case of a member of staff or volunteer, it is likely that suspension will take place at the point of referral to Police, whilst Police and internal procedures are being

Named person is responsible to the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where

### b. Other Incidents

There may be times when policy infringements could occur, through careless or irresponsible or deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- If a website search needs to be conducted (due to suspicion of inappropriate material) the DHP/DSL will contact the Network Manager with details and make a self-referral to PSG.
- Conduct the procedure using a designated computer that young people will not use and, if necessary, can be taken off-site by the police should the need arise. Use the same computer for the duration of the procedure (Deputy Head Pastoral device).
- It is important to ensure that the relevant staff have appropriate internet access to conduct the procedure and that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content. Once this has been completed and thoroughly investigated, the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by the Local Authority
  - Police involvement and/or action

### c. Illegal Incidents

- If the content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - promotion of terrorism or extremism
  - offences under the Computer Misuse Act
  - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state, may hinder a later police investigation.

All the above steps must be taken to provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The group should retain the completed form for future reference purposes.

## 14. School Actions and Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with proportionately as soon as possible and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with in line with the school behaviour policy.

## 15. Scope for the Policy

This policy applies to all school community members (including staff, pupils, volunteers, parents/carers and external hires) who have access to and are users of school digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable to regulate the behaviour of pupils when they are off the school site and empowers staff members to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying and other online safety incidents covered by this policy, which may take place outside of the school but are linked to membership of the school. The 2011 Education Act increased these powers regarding the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

## 16. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

### a. Governors

Governors are responsible for the approval of the online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Education Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Governor in charge of safeguarding (including online safety).

This role will include, where necessary:

- Regular meetings with the Deputy Head Pastoral (and DSL).
- Attendance at Online Safety Group meetings.
- Reviewing reports from the DHP about online safety incident logs.
- Reviewing reports from the DHP about the monitoring of filtering/change control logs.

### b. Head and Senior Leaders

The Head has a duty of care to ensure school community members' safety (including online safety). However, the Deputy Head Pastoral and DSL will delegate the day-to-day responsibility for online safety.
The Head and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed if a serious online safety allegation is made against a staff member.

The Head and the Deputy Head Pastoral ensure that the group in charge of online safety and other relevant staff receive suitable training to enable them to carry out their online safety roles.

### c. Deputy Head Pastoral (and DSL)

The Deputy Head Pastoral (and DSL) should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

a. sharing of personal data
b. access to illegal/inappropriate materials
c. inappropriate online contact with adults/strangers
d. potential or actual incidents of grooming
e. online-bullying

The Deputy Head Pastoral (and DSL) has:

a. day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school’s online safety policies/documents
b. ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident
c. liaises with the Local Authority
d. liaises with school technical staff

e. receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
f. meets regularly with Online Safety Governor and Online safety Group to discuss current issues, review incident logs and filtering/change control logs
g. attends relevant meetings of Governors
h. reports regularly to Senior Leadership Team

**d. Network Manager/Technical Staff**

Those with technical responsibilities are responsible for ensuring the following:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any relevant body online safety policy/guidance that may apply
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated regularly, and its implementation is not the sole responsibility of any single person (see "Technical Security Policy")
- that they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored so that any misuse/attempted misuse can be reported to the Head and Senior Leaders, Online Safety Lead (DSL), Online safety committee for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies
- Report on the above at the half termly E-Safety group meeting

**e. Teaching and Support Staff**

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the staff acceptable use policy/agreement
- they report any suspected misuse or problem to the Deputy Head Pastoral for investigation/action/sanction
- all digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students/pupils understand and follow the Online Safety Policy and acceptable use policies
- students/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned, students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Understand that school devices used at home should be password protected. Passwords should never be shared.

**Online Safety Group**

The Online Safety Group provides a consultative group with wide representation from the school community, responsible for issues regarding online safety and monitoring the Online Safety Policy, including the impact of initiatives. The group will also regularly report to the Governing Body.

Members of the Online Safety Group will assist the DSL with the following:

- The production/review/monitoring of the school's online safety policy/documents
- the production/review/monitoring of the school filtering policy and requests for filtering changes
- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/filtering/incident logs

- consulting stakeholders – including parents/carers/staff and the students/pupils about the online safety provision

**f. Students/Pupils**

- are responsible for using the school digital technology systems in accordance with the student/pupil acceptable use agreement
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on using mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and bullying
- should understand the importance of adopting good online safety practices when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school if related to their membership of the school

**g. Parents/Carers**

Parents/carers play a crucial role in ensuring their children understand the need to use the internet/mobile devices appropriately. The school will take every opportunity to help parents understand these issues through parents' evenings/coffee mornings, newsletters, letters, the school website, recommended websites, media and information about national/local online safety campaigns/literature and resources supplies and requested by '*Tooled up*'. Parents and carers will be encouraged to support the school in promoting good online safety practices, following guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/Learning Platform and online student/pupil records

## 17. Education & Training – Staff/Volunteers

All staff must receive online safety training and understand their responsibilities this policy outlines. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff via the SSS Training platform. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training during their induction programme, ensuring they fully understand the school's online safety policy and acceptable use agreements.
- The DSL will provide advice/guidance/training to individuals as required.

**Training – Governors**

The Governor responsible for safeguarding should participate in online safety training.

## 18. Community Users/External Hires

Visitors should not be allowed to access the school infrastructure. Where necessary, they should use the BYOD (Bring your own device) network and Guest login details can be provided upon request by the Network Manager.

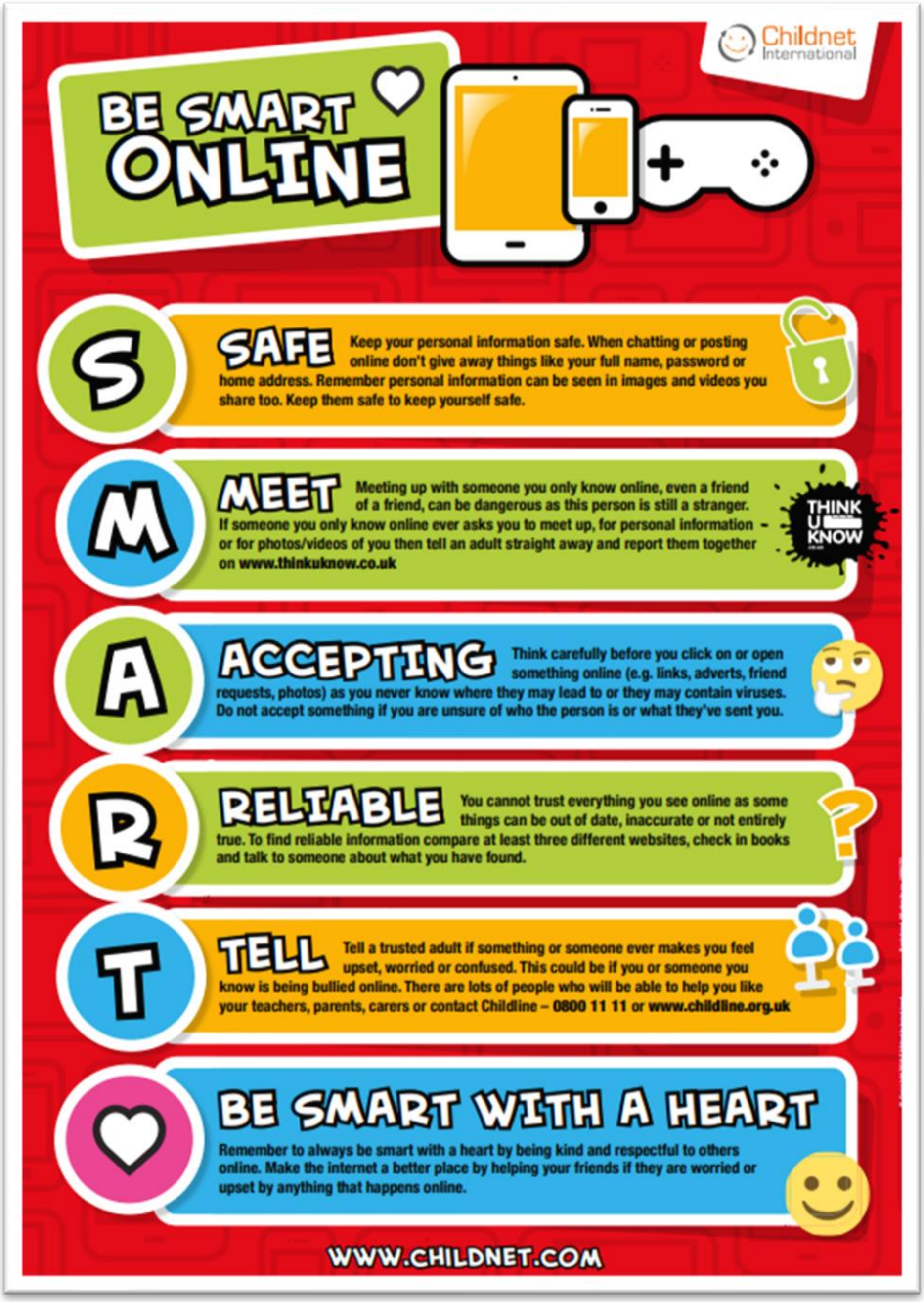
## 19. Technical – Infrastructure/Equipment, Filtering and Monitoring

The school will ensure that the school infrastructure/network is as safe and secure as possible, and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems, and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users from KS2 and above will be provided with a username and secure password by the Network Manager. They will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password.
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored.
- A clear process is in place to deal with requests for filtering changes.
- Internet filtering/monitoring should ensure children are safe from terrorist and extremist material when accessing the Internet.
- The school has provided enhanced/differentiated user-level filtering.
- School technical staff regularly monitor and record users’ activity on the school technical systems, and users are made aware of this in the acceptable use agreement.
- Orley Farm School uses ‘Smoothwall’ for our filtering, Firewall and monitoring services
- Orley Farm School uses ‘SENSO’ to monitor devices with OCR Reader for inappropriate images and language.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed – (immediate referral to the DSL & Network Manager).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc., from accidental or malicious attempts that might threaten the school systems and data security. These are tested regularly. The school infrastructure and individual devices are protected by up-to-date virus software.

**Appendix 1**

**BE SMART**



Childnet International

## BE SMART ONLINE

**S** **SAFE** Keep your personal information safe. When chatting or posting online don't give away things like your full name, password or home address. Remember personal information can be seen in images and videos you share too. Keep them safe to keep yourself safe.

**M** **MEET** Meeting up with someone you only know online, even a friend of a friend, can be dangerous as this person is still a stranger. If someone you only know online ever asks you to meet up, for personal information or for photos/videos of you then tell an adult straight away and report them together on **www.thinkuknow.co.uk**

THINK U KNOW

**A** **ACCEPTING** Think carefully before you click on or open something online (e.g. links, adverts, friend requests, photos) as you never know where they may lead to or they may contain viruses. Do not accept something if you are unsure of who the person is or what they've sent you.

**R** **RELIABLE** You cannot trust everything you see online as some things can be out of date, inaccurate or not entirely true. To find reliable information compare at least three different websites, check in books and talk to someone about what you have found.

**T** **TELL** Tell a trusted adult if something or someone ever makes you feel upset, worried or confused. This could be if you or someone you know is being bullied online. There are lots of people who will be able to help you like your teachers, parents, carers or contact Childline – **0800 11 11** or **www.childline.org.uk**

**BE SMART WITH A HEART** Remember to always be smart with a heart by being kind and respectful to others online. Make the internet a better place by helping your friends if they are worried or upset by anything that happens online.

WWW.CHILDNET.COM

## Appendix 2

### IT User Agreements

### Pre Prep:

### Acceptable use of the school's Devices and Internet: agreement for pupils and parents/carers

**Name of pupil:**

When I use the school's devices and get on the Internet in school, I will not:

- Use them without asking a teacher first or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Go on social networking sites (unless my teacher said I could as part of a lesson)
- Open any attachments in emails or click any links in emails without checking with a teacher first.
- Use mean or rude words when talking to other people online or in emails
- Share any photos without the consent of the person in the photo.
- Send any photos, videos, or live streams of people (including me) who aren't wearing all of their clothes, even if I have the consent of the person or people in the photo
- Share my password and personal details with others or log in using someone else's name or password
- Bully other people

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so they can help keep me and others safe and ensure I follow the rules.

I will tell a teacher or a staff member I know immediately if I find anything on a school computer or online that upsets me or is mean or wrong.

I understand that Artificial Intelligence (AI) should only be used if directed to by my teacher.

I understand that Artificial Intelligence (AI) must not be used in any way that would break plagiarism rules

I will respect all IT equipment belonging to the school and will always be responsible when I use the school's ICT systems and Internet.

I understand that the school can discipline me if I behave unacceptably online, even if I am not in school when I do so.

**Signed (pupil):** **Date:**

**Parent/carer agreement:** I agree that my child can use the school's ICT systems and Internet when appropriately supervised by a school staff member. I agree to the conditions set out above for pupils using the school's ICT systems and Internet and for using personal electronic devices in school, and I will make sure my child understands these.

**Signed (parent/carer):** **Date:**

**Middle School:**

## Acceptable use of the school's ICT facilities and Internet: agreement for pupils and parents/carers

**Name of pupil:**

When I use the school's devices and access the Internet in school, I will not:

- Use them without asking a teacher first or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Go on social networking sites (unless my teacher said I could as part of a lesson)
- Use chat rooms
- Open any attachments in emails or click any links in emails without checking with a teacher first.
- Use mean or rude language when talking to other people online or in emails
- Share any photos without the consent of the person in the photo.
- Send any photos, videos, or live streams of people (including me) who aren't wearing all of their clothes, even if I have the consent of the person or people in the photo
- Share my password and personal details with others or log in using someone else’s name or password
- Bully other people

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so they can help keep me and others safe and ensure I follow the rules.

I will tell a teacher or a staff member I know immediately if I find anything on a school computer or online that upsets me or is mean or wrong.

I understand that Artificial Intelligence (AI) should only be used if directed to by my teacher.

I understand that Artificial Intelligence (AI) must not be used in any way that would break plagiarism rules

I will respect all IT equipment in the school and will always be responsible when I use the school's ICT systems and Internet.

I understand that the school can discipline me if I do certain unacceptable things online, even if I am not in school when I do them.

| | |
|---|---|
| **Signed (pupil):** | **Date:** |

**Parent/carer agreement:** I agree that my child can use the school's ICT systems and Internet when appropriately supervised by a school staff member. I agree to the conditions set out above for pupils using the school's ICT systems and Internet and for using personal electronic devices in school, and I will make sure my child understands these.

| | |
|---|---|
| **Signed (parent/carer):** | **Date:** |

**Upper School:**

**Acceptable use of the school’s ICT facilities and Internet: agreement for pupils and parents/carers**

**Name of pupil:**

When using the school's devices (including Surface Go’s) and to access the Internet in school, I will not:

- Use them for a non-educational purpose (unless given permission by a teacher)
- Use them to break school rules
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails or follow any links in emails without first checking with a teacher.
- Use any inappropriate language when communicating online, including in emails.
- Share any photos without the consent of the person in the photo.
- Share any semi-nude or nude images, videos, or live streams, even if I have the consent of the person or people in the photo.
- Share my password or personal information with others or log in to the school's network using someone else's details.
- Bully other people

I understand that the school will monitor the websites I visit and my use of the school’s ICT facilities (including Surface Go’s) and systems.

I will immediately let a teacher or other staff member know if I find any material which might upset, distress or harm me or others.

I understand that Artificial Intelligence (AI) should only be used if directed to by my teacher.

I understand that Artificial Intelligence (AI) must not be used in any way that would break plagiarism rules.

I will respect all IT equipment in the school and always use the school's ICT systems and the Internet responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I am not in school when I do them.

**Signed (pupil):** **Date:**

**Parent/carer agreement:** I agree that my child can use the school's ICT systems and Internet when appropriately supervised by a school staff member. I agree to the conditions set out above for pupils using the school's ICT systems and Internet and for using personal electronic devices in school, and I will make sure my child understands these.

**Signed (parent/carer):** **Date:**

**Appendix 3**

**The Teaching of E-Safety Progression of Skills – Please click HERE**