Orleans Primary School

Online Safety Policy

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- [Relationships and sex education (RSE) and health education –
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the head of school and executive headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs

All governors will:

- Make sure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures

- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Head of School

The head of school is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the head in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the head, executive head and governing board to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the head of school, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the head of school and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a termly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and making sure that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by contacting the Head of School immediately.
- Following the correct procedures by speaking with the head of school if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to make sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the head of school of any concerns or queries regarding this policy
- Make sure that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

By the **end of primary school**, pupils will know:

- That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data are shared and used online
- How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE). This policy will also be shared with parents/carers.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the head of school and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the head of school.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and encourage them to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. [Class teachers] will discuss cyber-bullying with their classes and through assemblies and themed weeks. This will also be done through computing lessons. .

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The head of school and any member of staff authorised to do so by the Head of School or Executive Headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Head of School or Executive Headteacher
- Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the head of School] to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Orleans Primary recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Orleans Primary will treat any use of AI to bully pupils very seriously, in line with our behaviour policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in

cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

At Orleans Primary School, pupil safety and wellbeing are central to our approach and this policy outlines clear expectations around mobile phone use to support that goal.

- Only Year 6 pupils who travel to and from school independently and whose parents have provided written consent may bring a mobile phone onto school premises; all other year groups are not permitted to do so.
- Phones must be switched off at the school gate, handed to the class teacher for safe storage during the day, and collected at home time.
- Parents accept full responsibility for any loss, theft, or damage and are expected to discuss appropriate use with their child.
- Pupils must follow all rules, including keeping devices switched off and refraining from use on school grounds or during off-site activities.
- Misuse, including bullying, harassment, or inappropriate communication, will result in sanctions under the Behaviour Policy and potential withdrawal of phone privileges. This policy should be read in conjunction with the Mobile Phone (pupils) Policy for further guidance.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from from the School Business Manager.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour internet acceptable use . The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures / staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

11.1 Staff, governors and volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

11.2 Pupils

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering

● The risks of removable storage devices (e.g. USBs)

● Multi-factor authentication

● How to report a cyber incident or attack

● How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

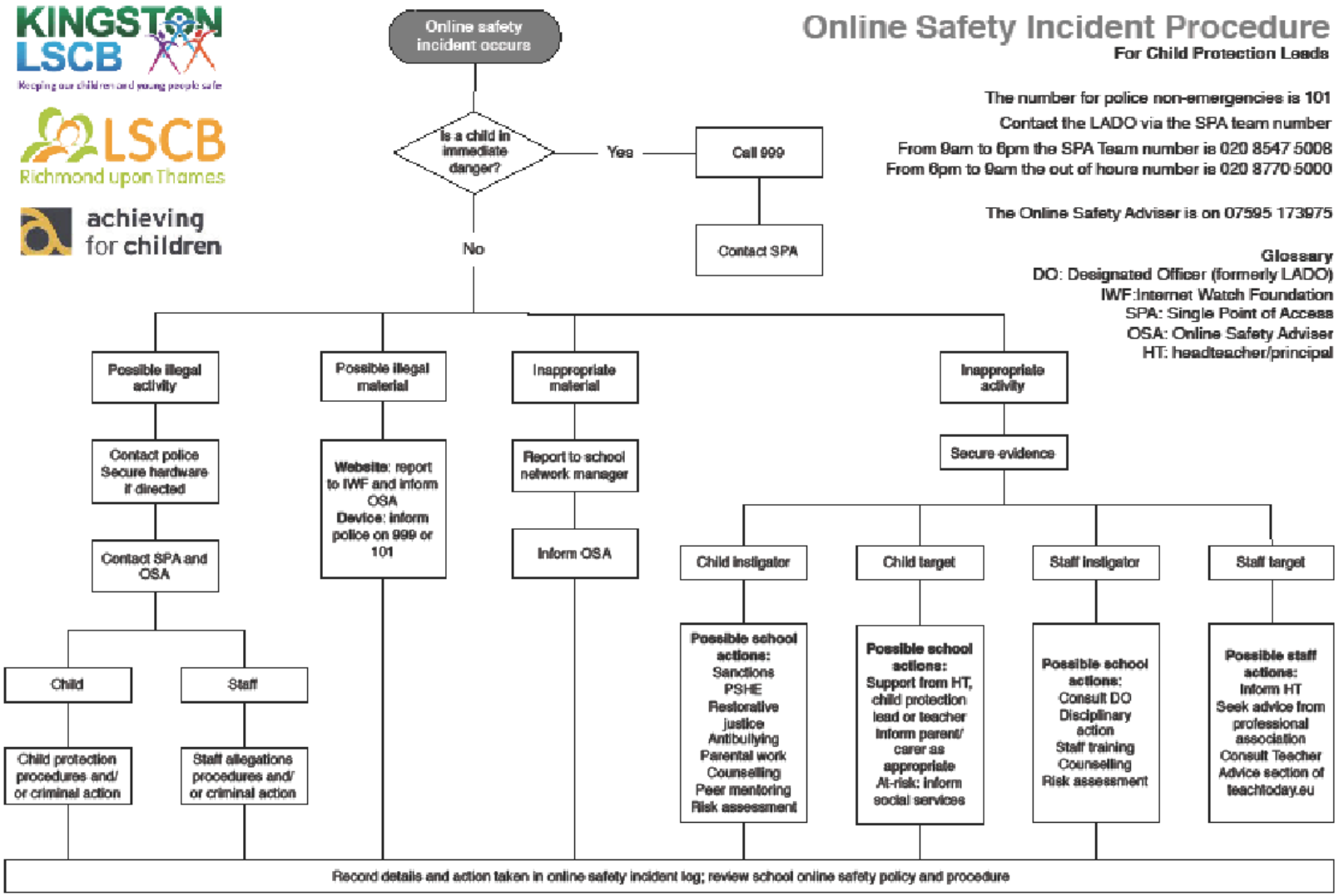
This policy will be reviewed every year by the DSL, Head of School and Executive Headteacher. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

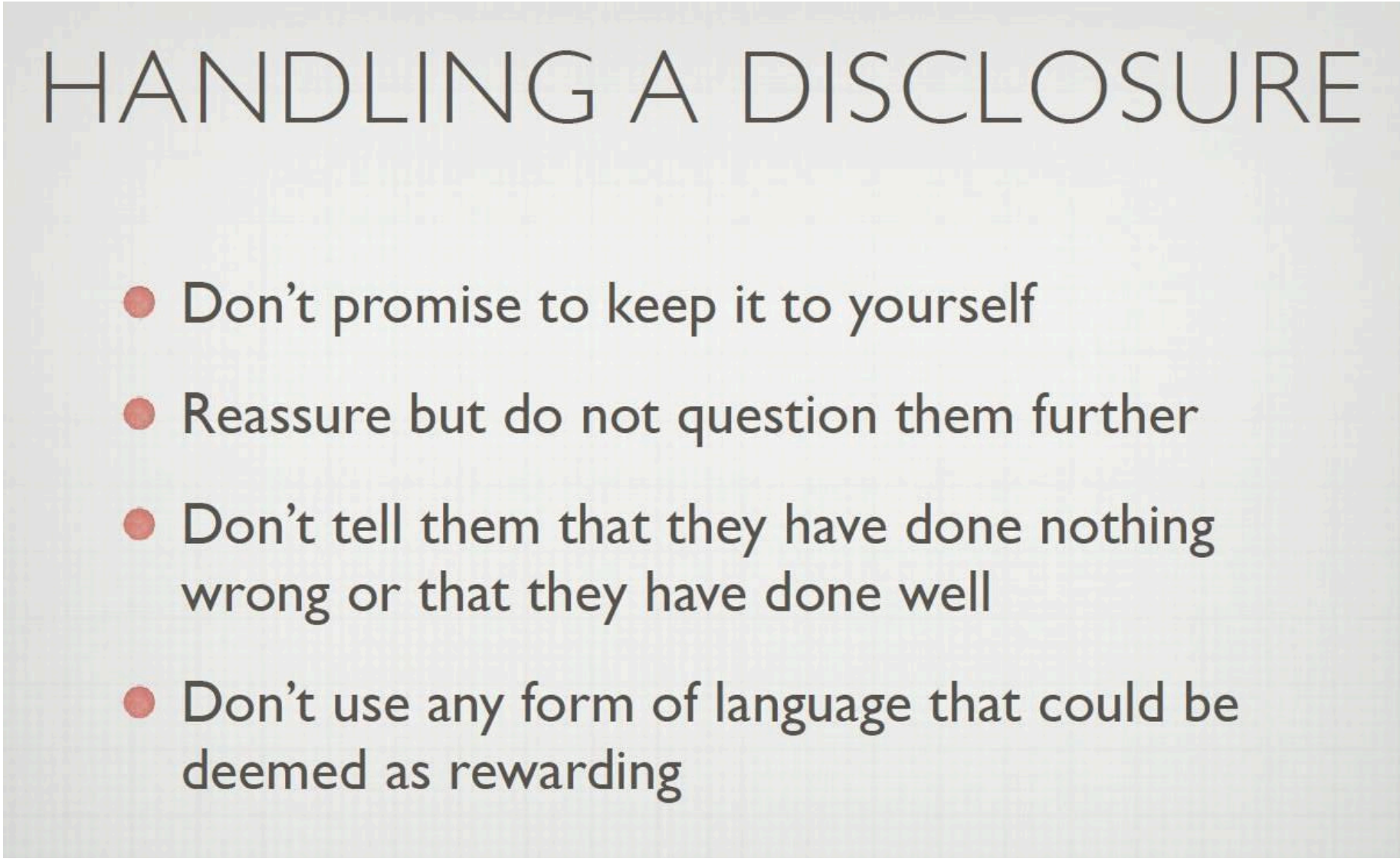
This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix A:


KINGSTON LSCB
Keeping our children and young people safe
LSCB
Richmond upon Thames
achieving for children
Online safety incident occurs
Is a child in immediate danger?
Yes
Call 999
Contact SPA
No
Online Safety Incident Procedure
For Child Protection Leads
The number for police non-emergencies is 101
Contact the LADO via the SPA team number
From 9am to 6pm the SPA Team number is 020 8547 5008
From 6pm to 9am the out of hours number is 020 8770 5000
The Online Safety Adviser is on 07595 173975
Glossary
DO: Designated Officer (formerly LADO)
IWF:Internet Watch Foundation
SPA: Single Point of Access
OSA: Online Safety Adviser
HT: headteacher/principal
Possible illegal activity
Possible illegal material
Inappropriate material
Inappropriate activity
Contact police Secure hardware if directed
Website: report to IWF and inform OSA
Device: inform police on 999 or 101
Report to school network manager
Secure evidence
Contact SPA and OSA
Inform OSA
Child Instigator
Child target
Staff Instigator
Staff target
Child
Staff
Possible school actions: Sanctions PSHE Restorative justice Antibullying Parental work Counselling Peer mentoring Risk assessment
Possible school actions: Support from HT, child protection lead or teacher Inform parent/ carer as appropriate At-risk: Inform social services
Possible school actions: Consult DO Disciplinary action Staff training Counselling Risk assessment
Possible staff actions: Inform HT Seek advice from professional association Consult Teacher Advice section of teachtoday.eu
Child protection procedures and/ or criminal action
Staff allegations procedures and/ or criminal action
Record details and action taken in online safety incident log; review school online safety policy and procedure

Appendix B:


HANDLING A DISCLOSURE
Don't promise to keep it to yourself
Reassure but do not question them further
Don't tell them that they have done nothing wrong or that they have done well
Don't use any form of language that could be deemed as rewarding

Appendix C 1:

Acceptable Use: Staff

The use of ICT resources must be in support of the role you perform for the School. You are personally responsible for this provision at all times when you use any of the ICT resources.

By using any The School IT equipment after reading this ICT user Agreement means that you understand and accept these terms and conditions listed below Any breach of these conditions may have disciplinary consequences.

1. I understand that WhatsApp (or similar messaging platforms) is not an approved communication channel for the School. As this is not a School-controlled platform, The School is not able to monitor or easily access the information held. This can cause issues if there were to be a Subject Access or Freedom of Information Request. Any existing WhatsApp group containing staff should not show any affiliation with the School via the name. The approved communication channels are School email or the messaging function within Tapestry or google classroom.
2. I will comply with the ICT system security and not disclose any passwords provided to me by the School or other related authorities.
3. My passwords will be "strong" in nature, and include capitals, lower case, number, and symbol and be of least 8 characters long. If I suspect it has been compromised, then I will change it immediately.
4. I will ensure that I am the only one who uses my user account and understand that anything undertaken while I am logged in, I will be held responsible for.
5. I will lock my computer screen whenever I leave it unattended.
6. I will not autosave my password or log in details for any of the School systems, as this negates the effectiveness of the password.
7. I will ensure that all electronic communications are compatible with my professional role.
8. If I receive a suspicious email, I will report it to the school business manager before clicking on any links, downloading any attachments or entering my user details. I will not forward the email unless instructed by the IT support contractor or school business manager.
9. My personal social media accounts will not show a direct link with the School and I understand that whatever I post can be seen, therefore if I am identifiable content will be of a professional nature.
10. I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff unless agreed with SLT. There are strictly limited exceptions to this, for example when the technology protects or keeps children safe or when there is direct relevance to a lesson. Even when used for these purposes, staff should never give the impression that it is being used casually or for personal use. I will not store any such images or videos at home.
11. I agree and accept that any computer or laptop loaned to me by the School is provided solely to support my professional responsibilities and that I will notify the School of any "significant personal use" as defined by HM Revenue & Customs. Under no circumstances should the operating system or installed applications on any School provided devices be modified by the user in any way.
12. I will only use the approved, secure email system for any school business and will always check if I should be Cc'ing Bcc'ing recipients and that the correct email address, and attachment has been selected.

13. I will ensure that personal data is kept secure and is used appropriately, whether in the office, or when working remotely and in accordance with the School's Data Protection Policy.
14. I will transfer personal data by email securely and consult with the IT support contractor or school business manager to verify appropriate platforms to complete this task.
15. I understand that anything I write in an email or document about an identifiable person can be requested via a Subject Access Request and read by that individual. Therefore, I would not write anything that I would not want that person to read, could bring the School in disrepute or is counter to the staff code of conduct.
16. I will not install any hardware or software without the permission of the IT Department.
17. I will consider if the communications I send breach confidentiality or the Data Protection Act, by asking "should the recipient view this information".
18. I understand that I can cause a data protection breach by destroying or corrupting data and all data should be held in line with the School's Data Retention Policy.
19. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
20. I will support the School's approach to online safety which is detailed in its Online Safety Policy.
21. I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Senior Leadership Team.
22. I will respect copyright and intellectual property rights and will ensure that any images that I use are not subject to copyright. These include images found on internet searches.
23. I will ensure that my online activity, both in work and outside work, will not bring the School, my professional reputation, or that of others, into disrepute.
24. I will not use the School's ICT systems for any commercial activities, such as work for a for-profit organisation.
25. When using personal devices please ensure that the device has anti-virus in place that has been updated to limit potential vulnerabilities.
26. We appreciate that others may use the personal devices you use to access the system with; however please ensure that you are the only person who can access your user accounts and that you understand that anything undertaken while you are logged in, will be considered done by you.
27. I will only use School approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the staff-only drive within School.

Artificial Intelligence (Addendum)

As technology evolves, including the use of Artificial Intelligence (AI) tools, it is essential that all school staff adhere to the following guidelines to ensure compliance with Data Protection regulations, safeguarding policies, and responsible ICT use. This addendum aligns with UK GDPR requirements and Orleans Primary School's data protection policies.

Data Protection & GDPR Compliance

- Free AI tools may process and store data using global infrastructure that falls outside UK GDPR jurisdiction.
- Submitting any Personally Identifiable Information (PII), sensitive school data, or identifiable student/staff content can result in data protection breaches.
- Always anonymise any data before entering it into any AI tool or external platform.

Appendix C2

CONTRACTOR, GOVERNOR AND VISITOR ACCEPTABLE USE POLICY

IT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Jane Evans, the Designated Safeguarding Lead for the School.

- I will only use the school's email/Internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head of school or Governing Body.
- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
- Under no circumstances will I share my log in details for the pc, email or any school software with other members of staff. Staff must only use their own log ins.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, personal email address and social media platforms to pupils.
- I will only use the approved, secure email system(s) for any school business - USO-FX.
- I will ensure that personal data and sensitive information (such as data held on Integris or on laptops) is kept encrypted and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not use Data/Memory Sticks to store any information related to school.
- Personal data can only be taken out of school or accessed remotely when authorised by the head of school and executive headteacher or Governing Body.
- Personal data must not be emailed to personal email accounts.
- I will not install any hardware or software without the permission of the DSL.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will not use my mobile phone for personal reasons in sight of children and will respect my colleagues when using it in private.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Headteacher.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will support the school's approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I will respect Copyright and Intellectual Property Rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's Online-Safety Policy and help pupils to be safe and responsible in their use of IT and related technologies.
- I will not use personal devices to take images or films of children at school.

User Signature
I agree to follow this Code of Conduct and to support the safe use of IT throughout the School.

Signature…….. Date……

Appendix D:

	Autumn 1	Autumn 2	Spring 1	Spring 2	Summer 1	Summer 2
Nursery	Online Safety Intro to Equipment and Safe Use. Remote Control Toys JiT Busy Things					
Reception	Online safety Using a computer (Kapow)		All about Instructions (Kapow) Safer Internet Day	Exploring hardware (Kapow)	Programming Beebots and Codapillars (Kapow)	Introduction to Data Handling (Kapow)
Year 1	Online Safety (Kapow)	Improving Mouse Skills (Kapow)	Keyboard Skills - Busy Things Safer Internet Day	Programming BeeBot (Kapow)	Algorithms Unplugged (Kapow)	Introduction to Data (Kapow)
Year 2	Online safety (Kapow)	What is a Computer? (Kapow)	Algorithms and Debugging (Kapow) Safer Internet Day	International Space Station (Kapow)	Keyboard Skills - Dance Mat Typing	Word Processing (Kapow)
Year 3	Online safety – cyber pass (Kapow)	Networks and the Internet (Kapow)	Programming Scratch (Kapow) Safer Internet Day	Touch Typing (Englishtype.)	Journey inside a Computer (Kapow)	Video Trailers (Kapow)
Year 4	Online safety – cyber pass (Kapow)	Collaborative Learning (Kapow)	Further Coding with Scratch (Kapow) Safer Internet Day	HTML (Kapow)	Computational Thinking (Kapow)	Touch Typing (Englishtype.)
Year 5	*Online safety – cyber pass* (Kapow)	Search Engines (Kapow)	Programming Music - Scratch (Kapow) Safer Internet Day	Mars Rover 1 (Kapow)	Touch Typing (Englishtype.)	Programming Crumble Robots
Year 6	*Online safety – cyber pass* (Kapow)	*Bletchley Park* (Kapow)	Touch Typing (Englishtype.) Safer Internet Day	Intro to Python (Kapow)	Big Data 1 (Kapow)	History of Computers (Kapow)

Online Safety Computing Systems and Networks Programming Data Handling Skills Showcase Creating Medi

Appendix E Pupil Agreements
ACCEPTABLE USE AGREEMENT KEY STAGE ONE PUPILS
My name is _____

To stay **SAFE online and on my devices**:	
1. I only **USE** devices or apps, sites or games if a trusted adult says so	
2. I **ASK** for help if I'm stuck or not sure	
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused	
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult	
5. I look out for my **FRIENDS** and tell someone if they need help	
6. I **KNOW** people online aren't always who they say they are	
7. Anything I do online can be shared and might stay online **FOREVER**	
8. I don't keep **SECRETS** or do **DARES AND CHALLENGES** just because someone tells me I have to	
9. I don't change **CLOTHES** in front of a camera	
10. I always check before **SHARING** personal information	
11. I am **KIND** and polite to everyone	

My trusted adults are:

_____ at school, _____ at home

For parents/carers

To find out more about online safety, you can read Orleans Primary School's full Online Safety Policy at **www.orleans.richmond.sch.uk** for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc).

You can find support and online safety resources for parents at parentsafe.lgfl.net

ACCEPTABLE USE AGREEMENT KEY STAGE TWO PUPILS

This agreement will help keep me safe and help me to be fair to others

1. ***I learn online*** – I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. School internet and devices are monitored.
2. ***I ask permission*** – Whether at home or school, I only use the devices, apps, sites and games I am allowed to, at the times I am allowed to.
3. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things.
4. ***I am a friend online*** – I won't share anything that I know another person wouldn't want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
5. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
6. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes addons can cost money, so it is important I always check for these too.
7. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
8. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
9. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
10. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
11. ***I check with an adult before I meet an online friend*** face to face for the first time, and I never go alone.
12. ***I don't do live videos (live streams) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
13. ***I keep my body to myself online*** – I never get changed or show what's under my clothes in front of a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.

14. ***I say no online if I need to*** – I don't have to do something just because a friend dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
15. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
16. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
17. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
18. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour.
19. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
20. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
21. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
22. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.

I have read and understood this agreement. If I have any questions, I will speak to a trusted adult:

At school that includes _____

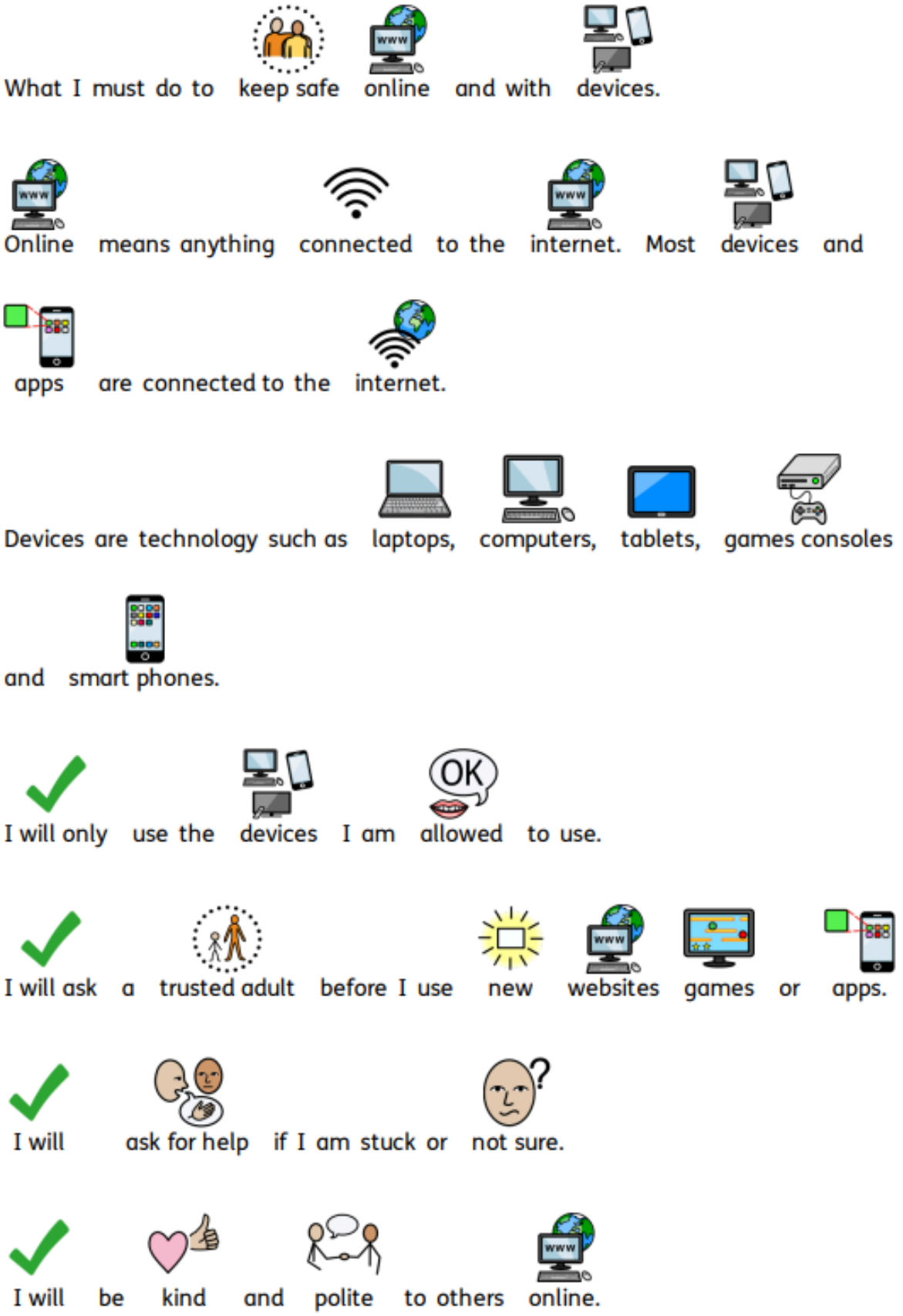
Outside school, my trusted adults are_____

Signed: _____ **Date: _____**

For parents/carers

If your parents/carers want to find out more, they can read Orleans Primary School's full Online Safety Policy at www.orleans.richmond.sch.uk for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc). They will also have been asked to sign an AUP for parents.

ACCEPTABLE USE AGREEMENT SEND PUPILS (Example that will be adapted according to pupil need)




I will tell a trusted adult if I feel worried, scared, nervous, sad,


angry or embarrassed when using a device online.

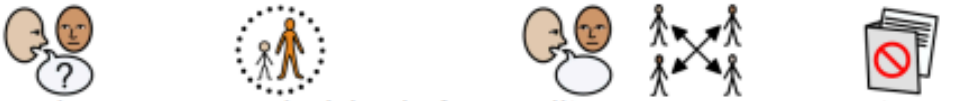

I will tell a trusted adult if I feel unsafe when using a device online.


I know people online sometimes tell lies.


They might lie about who they are or where they live.


I never have to keep secrets from my trusted adults.


I will not change clothes or undress in front of a webcam.


I will always ask a trusted adult before telling anyone my private


information or my location.


I know that anything I  say or do  online may be there forever. It can

be given to my  family, my  friends or  strangers.

This could make  me  feel sad or  embarrassed.

My  trusted adults at  school are _____

My  trusted adults at  home are _____

My  name is _____

Appendix F: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyberbullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	