

# Orleans Primary School



## Online Safety Policy

Governor's Committee Responsible	P, C&C
Status	Non-statutory
Review Cycle	Annual
Date written/last review	September 2021
Date of next review	September 2022

This policy has been reviewed in line with the updated Keeping Children Safe in Education (2021) document and is part of the schools statutory Safeguarding Policy. Any issues and concerns with online safety must follow the schools safeguarding processes. This policy has also been reviewed to make reference to Covid-19 and the use of technology at home.

The school has also utilised the DFE document 'Teaching Online Safety within Schools' June 2019.

Signed Headteacher:

Date:

Signed Chair of P,C&C:

Date:

## Online Safety Policy – Contents Page

Content	Page Number
1. Content and Rationale	3
2. Scope of the Policy	3
3. Whole School Approach to the Use of ICT	4
4. Roles and Responsibility 4.1 Governors 4.2 Designated Safeguarding Lead 4.3 Headteacher and other Senior Leaders 4.4 The role of Technical Support 4.5 All Staff, Including Contractors and Agency Staff, and Volunteers 4.6 Visitors and the Role of the Community 4.7 Pupils 4.8 Parents and Carers	4
5. Specific Risks	7
6. Curriculum – Educating Pupils about Online Safety 6.1 Educating Parents about Online Safety	7
7 Cyber-Bullying 7.1 Definition 7.2 Preventing Online/Cyber-Bullying at Orleans Primary School 7.3 Dealing with Alleged Incidents of Cyber-bullying 7.4 Examining Electronic Devices	8
8 Acceptable Usage	9
9 Pupils Mobile Phone /Electronic Devices in School	9
10 Staff Using Mobile Devices Outside of School	10
11 How the School will Respond to Issues of Misuse	10
12 Training	11
13 Monitoring Arrangements	11
14 Process for Managing the Internet Safely	11
15 Copyright and Plagiarism	13
16 Password Policy	13
17 Managing Email	13
18 The Use of Digital and Video Images	14
19 Managing Equipment	14
Appendix A – Online Safety Process for Dealing with Incidents	16
Appendix B – Handling a Disclosure	17
Appendix C – Staff Governor, Visitors, Contractors Acceptable Usage Policy	18
Appendix D – Computing Curriculum Map	20
Appendix E – Pupil Acceptable Usage Agreements	21
Appendix F – Online Safety Staff Training Needs Audit Form	27
Appendix G - Online Safety Incident Report Log	28
Appendix H – Contact Details for Social Networking Sites	29

## **1. Context and Rationale:**

At Orleans Primary School online safety is an integral part of our safeguarding culture. As such we ensure that all staff members are trained in knowing how to recognise online safeguarding issues and the procedures to follow should an issue arise. The staff and Governors of Orleans Primary School recognise they have a duty to ensure that all pupils are able to make a valuable contribution to society and this is only possible to achieve if we ensure that pupils develop and apply their ICT capability effectively in their everyday lives.

The school is aware of its responsibilities in ensuring that ICT usage by all network users is responsible, safe and secure. There are relevant and comprehensive policies in place which are understood and adhered to by network users.

It is the duty of the school to ensure that every child in their care is safe, and the same principles apply to the 'virtual' or digital world as would be applied to the school's physical buildings. This policy document is drawn up to protect all parties - the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements of school policy.

## **2. Scope of the Policy**

This policy applies to all members of the school community (including staff, pupils, Governors, volunteers, Parents / Carers, visitors, community users) 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 members of staff to impose sanctions for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the schools own published Behaviour Policy.

The school will deal with such incidents within this policy and associated Behaviour and Anti-Bullying Policies and will, where known, inform Parents /Carers of incidents of inappropriate online safety behaviour that take place out of school.

This Online Safety Policy is linked to our:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti bullying Policy
- Staff disciplinary procedures
- Data Protection Policy and privacy notices
- Complaints Procedure
- Staff Code of Conduct and Acceptable Usage Policies
- PupilMobile Phone/Devices Policy
- Pupil Acceptable Usage Agreements

### **3. Whole School Approach to the Safe Use of Technology**

This policy has been created by the Senior Leadership Team of Orleans Primary School and is reviewed on an annual basis.

Creating a safe technological learning environment includes four main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive online safety education programme for pupils, staff and parents.
- Creating a safe online/remote learning environment.

### **4. Roles and Responsibilities**

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

#### **4.1 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 Governors P, C & C Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor as part of their role as a Safeguarding Governor (Alex Axiom).

The role of the Online Safety Governor will include:

- Regular monitoring of online safety incident logs.
- Regular monitoring of filtering.
- Reporting to relevant Governor Committee meetings.
- Agree and adhere to the terms on acceptable usage of the schools ICT systems and the internet.

#### **4.2 Designated Safeguarding Lead**

Details of the school's Designated Safeguarding Lead (DSL) and Deputy DSLs are set out in our Safeguarding and Child Protection Policy.

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

- In ensuring that staff understand this policy, and that it is being implemented consistently across the school.
- Working with, ICT support (Click on It) and other staff, as necessary to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged (see appendix G) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Behaviour Policy.
- Updating and organising/delivering staff training on online safety (appendix F is the online safety audit with use with staff to identify online safety training needs.)
- Liaising with outside agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Governing Body.

The DSL should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from the four areas of risk as categorized by the DFE in KCSIE\* 2021:

- **Content**; being exposed to illegal, inappropriate or harmful content, for example; pornography, fake news, racism, misogyny, self harm/suicide, anti-semitism, radicalisation and extremism.
- **Contact**: being subjected to harmful online interaction with other users for example peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention of grooming or exploiting them for sexual, criminal, financial or other purposes.
- **Conduct**: personal online behaviour that increases the likelihood or causes, harm, for example making, sending and receiving explicit images (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.

This also includes:

- Sharing of personal data.
- Access to illegal / inappropriate materials.
- Inappropriate on-line contact with adults / strangers.
- Potential or actual incidents of grooming .
- Online-bullying.
- Monitoring incident logs.
- Consulting stakeholders – including parents / carers and the students / pupils about the online safety provision.
- Monitoring improvement actions identified through use of the 360-degree safe self-review tool.

#### **4.3 Headteacher and Senior Leaders:**

The Headteacher/DSL is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

#### **4.4 The role of Technical Support:**

Orleans Primary School has a contract with 'Click on IT' who provide our technical support. Their role is to ensure:

- 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 Local Authority guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- The filtering system is appropriate, applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person within their company.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network, internet, remote access, email is regularly monitored in order that any misuse attempted misuse can be reported to the Headteacher/ DSL for investigation.
- That monitoring software / systems are implemented and updated as agreed in school.

This list is not intended to be exhaustive and it is the role of Technical Support to bring to the attention of the school any new developments relating to the safety and security of the school.

#### **4.5 All Staff are Responsible for Ensuring that:**

- They utilise their Safeguarding training (last carried out September 2021 with all staff) in relation to dealing with any online safety safeguarding concerns.
- They have an up to date awareness of online safety matters through participating in training and that they have read the current school Online Safety Policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy (this is section 2 within our Staff Code of Conduct).
- They report any suspected misuse or problem to the DSL for investigation.
- All digital communications with 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.
- Pupils understand and follow the Online Safety Policy and Acceptable Usage Agreements.
- 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 with regard to these devices.
- In lessons where internet use is pre-planned, 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.

#### **4.6 Visitors, volunteers and members of the school community:**

Visitors, Volunteers and members of the community who use the schools ICT systems or internet will be made aware of this policy, when relevant, and expected to follow it. If appropriate, they will be expected to agree to the terms of acceptable use.

#### **4.7 Pupils:**

The school includes online safety in our curriculum and we ensure that every pupil has been educated about safe and responsible use. (Please see Appendix D for our Computing Curriculum Map).

Pupils:

- Are responsible for using the school and remote online learning technology systems in accordance with the Pupil Acceptable Use Agreement.
- Pupils need to know how to control and minimise online risks and how to report a problem.
- 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 the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying including peer on peer abuse such as up skirting.
  - Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.
  - Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

#### **4.8 Parents / Carers:**

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help Parents understand these issues through Parents' Evenings, newsletters, letters, the Orleans Primary School website and 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:

- Digital and video images taken at school events.
- Access to Parents' sections of the website and on-line pupil assessment systems i.e. Tapestry.
- Their children's personal devices in the school.

5. Parents can seek further advice on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: <https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>
- Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>
- Parent factsheet, Childnet International: <https://www.childnet.com/parents-and-carers>
- Parent Information on Online Sexual Harassment: <https://www.childnet.com/resources/online-sexual-bullying-advice-for-parents-and-carers-of-9-12-year-olds>

Parents can report any concerns they have regarding anything which has happened outside school via CEOP: <https://www.ceop.police.uk/Safety-Centre/>

## **6. Curriculum - Educating Pupils about Online Safety**

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

In Early Years, pupils will be taught to use equipment safely and the importance of telling an adult if they are worried about anything.

In Key Stage 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.

In Key Stage 2, pupils will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about connect and contact.

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

The school will use assemblies to raise pupil's awareness of the dangers that can be encountered online and may invite speakers to talk to pupils about this either in assembly or during lessons.

### **6.1 Educating Parents about Online Safety**

The school will raise Parents' awareness of internet safety in letters or other communications home and in information via our school website. This policy will also be shared with parents. The school will ask for a parent volunteer to join the Online Safety Group.

**Online Safety will also be covered during Parents Curriculum Evenings.**

If parents have any questions or concerns in relation to online safety, these should be raised in the first instance with the Headteacher/DSL.

## **7 Cyber-Bullying**

### **7.1 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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Behaviour Policy and the School Mobile Phone/Devices Policy). Children can abuse each other (sometimes referred to as Peer-on-Peer Abuse) and this can take the form of cyber-bullying, this can have a lasting emotional impact on a child/ren.

### **7.2 Preventing Online/Cyber-Bullying at Orleans Primary School**

We take any form of bullying very seriously and will take swift action to deal with any such incidents. The Headteacher/DSL will investigate the report of any online bullying and will take appropriate action as set out in our Behaviour and Discipline Policy.

To help prevent cyber-bullying, we will ensure that pupils understand what cyber-bullying 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 are encouraged 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 class groups, and the issue will be addressed in assemblies.

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 Relationships, Health and Sex Education (RHSE), 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.

The school offers a comprehensive package of information to parents and carers to support them in knowing how to keep their children safe online. This includes regular information such as support in setting up parental controls on electronic devices, an annual parent Online Safety Meeting with a specialist Online Safety Advisor. Prior to pupils moving to year 6 the school organises an information meeting for Year 5 parents and pupils to provide advice about how to keep safe online when the pupils are allowed to bring a phone to and from school. The school also sends information/leaflets on cyber-bullying to Parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

### **7.2 Dealing with Alleged Incidents of Cyber-Bullying**

In relation to a specific incident of cyber-bullying, the school will follow the procedures as set out in our Behaviour and Discipline 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. (Please see Appendix A for flow chart)



The DSL will consider whether the incident should be reported to the Police if it involves illegal material, and will work with external services if it is deemed necessary to do so. Parents will be informed and asked to attend a meeting at school with the Headteacher/DSL.

## **7.2 Examining Electronic Devices**

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the Senior Leadership Team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the Police.

Any searching of pupils will be carried out in line with the DfE's latest guidance on

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/674416/Searching\\_screening\\_and\\_confiscation.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674416/Searching_screening_and_confiscation.pdf)

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

## **8. Acceptable Usage**

All pupils, Parents, staff, long-term volunteers and Governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems, personal devices and the internet (appendices E1 and E2). Visitors will be expected to read and agree to the school's terms on acceptable use.

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.

More information is set out in the Acceptable Use Agreements in appendix E. (Please note Acceptable Usage Agreements will be updated as necessary during the academic year.)

## **9. Pupils Using Mobile Phones in School (Please also see Mobile Phone/Devices Policy)**

Only year six pupils may bring mobile phones into school. They are not permitted to use them at any time during the school day. Year 6 pupils are only permitted to bring mobile phones when parents have signed the mobile phone agreement. Any breach of the Acceptable Use Agreement by a pupil will trigger disciplinary action in line with the school Behaviour Policy, which may result in the confiscation of their device.

Pupils are not permitted to bring any other devices such as ipads, tablets or game consoles into school at any point.

No pupil within any other year group is permitted to bring a mobile phone or any other mobile device into school and staff will confiscate these if they are found. Parents will be contacted and asked to collect the phone or any other device from the school office.

#### **10. Staff Using Mobile Devices Outside of School**

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's Acceptable Usage Policy as set out in appendix C.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Staff are not permitted to use USB devices containing data relating to the school.

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

Work devices must be used solely for work activities.

#### **11. How the School will Respond to Issues of Misuse of ICT Systems**

Where a pupil misuses the school's ICT systems, Internet or social media, we will follow the procedures set out in the Behaviour and Discipline Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff (including Governors) and pupils are given information about infringements in use and possible sanctions.

Sanctions available include:

- interview/counselling by Deputy Head / Headteacher;
- informing Parents or Carers;
- removal of Internet or computer access for a period, (which could ultimately prevent access to files held on the system);
- referral to LA / Police.

Our DSL acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher. The Headteacher will follow the Online Safety Escalation Protocol (see appendix A).

Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy.

Complaints related to child protection are dealt with in accordance with school / LA child protection procedures. (see appendix A).

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. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

## **12. Training**

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).

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 Safeguarding and Child Protection Policy.

## **13. Monitoring Arrangements**

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

This policy will be reviewed annually by the DSL. At every review, the policy will be shared with the Governing Board.

## **14. Process for Managing the Internet Safely**

### **The Risks**

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be considered inappropriate and restricted elsewhere. In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk.

### **Technical and Infrastructure:**

This school:

Maintains the filtered broadband connectivity through the LGfL and so connects to the 'private' National Education Network;

- Works in partnership with the LA to ensure any concerns about the system are communicated to LGfL so that systems remain robust and protect pupils;
- Ensures their network is 'healthy' by having health checks annually on the network;
- Utilises caching as part of the network set-up;
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies;
- Ensures the Systems Administrator / network manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Never allows pupils access to Internet logs;
- Never sends personal data over the Internet unless it is encrypted or otherwise secured;
- Uses 'safer' search engines with pupils where appropriate

This school:

- Supervises pupils' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older pupils have more flexible access;
- Uses the pan-London LGfL / Atomwide filtering system which blocks sites that fall into categories such as pornography, race hatred, radicalisation, child sexual exploitation, gaming, sites of an illegal nature;
- Staff preview all sites before use [where not previously viewed and cached] or only use sites accessed from managed 'safe' environments;
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs users that Internet use is monitored;
- Informs staff and pupils that they must report any failure of the filtering systems directly to the ICT leader. Our systems administrators report to LA / LGfL where necessary;
- Only uses approved or checked webcam sites;
- Keeps a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures the named DSL has appropriate training;
- Makes information on reporting offensive materials, abuse / bullying etc. available for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police/LA;
- Adheres to our Safeguarding policy when a child makes a disclosure (See Appendix B).

## **Education and Training:**

This school:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher or responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or System Manager;
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report abuse;

- Has a clear, progressive online safety education programme throughout all Key Stages, built on LA / London / national guidance.

Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

- to STOP and THINK before they CLICK;
- to discriminate between fact, fiction and opinion;
- to develop a range of strategies to validate and verify information before accepting its accuracy;
- to skim and scan information;
- to be aware that the author of a web site / page may have a particular bias or purpose and
- to develop skills to recognise what that may be;
- to know some search engines / websites that are more likely to bring effective results;
- to know how to narrow down or refine a search;
- to understand how search engines work;
- to understand 'Netiquette' behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand how to make the right decisions and keep themselves safe and happy when using the digital world in their relationships;
- to understand why they must not post pictures or videos of others without their permission;
- to know not to download any files - such as music files - without permission;
- to have strategies for dealing with receipt of inappropriate materials.

## **15. Copyright and Plagiarism**

This school;

- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright/intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial side of the internet, as age appropriate. This may include, risks in pop ups; buying online, online gaming/gambling.
- Ensures staff know how to encrypt data where the sensitivity requires that they understand data protection and general ICT security issues linked to their role and responsibilities;
- makes training available to staff on the online safety curriculum.

## **16. 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 and to change them at least twice a year.

- Staff are trained to logout of any machine when leaving it unattended.

## **17. Managing E-mail**

E-mail is now an essential means of communication for staff in our schools and increasingly for pupils and homes. This school:

- does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for any communication with the wider public.
- Contacts the police if one of our staff receives an e-mail that we consider is particularly disturbing or breaks the law.
- Manages accounts effectively, with up to date account details of users.
- Reports messages relating to or in support of illegal activities.
- Staff use the LGfL e-mail systems for professional purposes.

## **18. Use of Digital and Video Images**

In this school:

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained.
- Uploading of information is restricted to the website team.
- The school website complies with the school's statutory requirements.
- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities is not published.
- Photographs of children published on the web site do not have full names attached;
- 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;
- Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are deleted at the end of the year - unless an item is specifically kept for a key school publication;
- We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website.
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Pupils are taught about how images can be abused in their online safety education programme;
- The school does not allow Parents/Carers/volunteers or visitors to the school to take photos of pupils at any time without specific permission. Further clarification can be found in our Social Media Policy.

## **19. Managing Equipment**

The computer system / network is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

***The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.***

To ensure the network is used safely this school:

- Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find;
- Makes clear that pupils should never be allowed to log-on or use teacher and staff logins - these have far less security restrictions and inappropriate use could damage files or the network;

- Makes it clear that no one should log on as another user - if two people log on at the same time this may corrupt personal files and profiles;
- 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.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;
- Maintains equipment to ensure Health and Safety is followed;
- 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; Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their USO;
- 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 LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Reviews the school ICT systems regularly with regard to security.

#### **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 handheld device brought into school.
- Staff members may use their phones during school break times (preferably not taking or making personal phone calls in the staff room so that it remains a whole staff usage area). 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.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

## Appendix A:

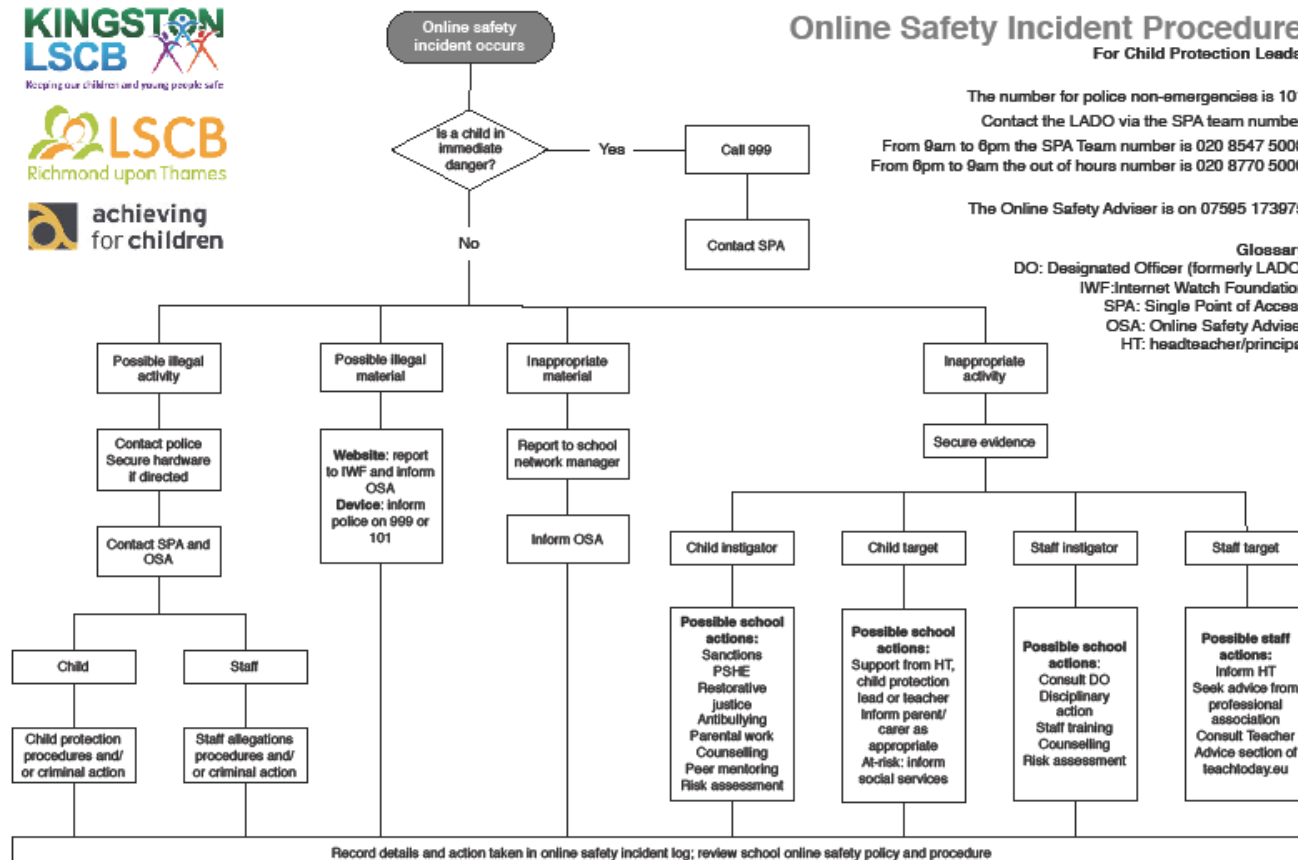


## Online Safety Incident Procedure For Child Protection Leads

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





# 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:

### Part B: STAFF, 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 Headteacher 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 Integriss 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 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/carers, 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 using safely. Remote control toys  Busv Things					
Reception	Computing systems 1  Online safety Using a computer		Programming 1.  All about instructions	Computing systems 2.  Exploring hardware	Programming 2.  Programming <del>Beebots</del> and <del>Codapillars</del> .	Data handling  Introduction to data handling
Year 1	Online safety Computer Rules	Logging on Mouse skills	Pictograms (Online safety)	Charts	Information around us Keyboard skills	Algorithms Blue Bots & Turtle
Year 2	Online safety Logging on and keyboard skills	Using Graphs to answer questions	Jit – turtle (online safety)	Algorithms Blue bots & tactile readers	Jit animate	Word processing - writing stories
Year 3	Online safety – cyber pass Internet Research	Networks	Programming code.org (online safety)	Programming Scratch <del>InOBots</del>	Communication Word processing	Multimedia Video performance
Year 4	Online safety – cyber pass Comic Strips	Programming Animation	Email and networks (online safety)	Programming	Blogging (Word & image)	Data Logging (excel)
Year 5	<i>Online safety</i> – <i>cyber pass</i> Good internet research	Data handling (infographics)	The school network (online safety)	Web design Binary	Programming Crumble robots	Programming Scratch – <i>Developing Games</i>
Year 6	<i>Online safety – cyber pass</i> Digital literacy –plagiarism – trusted sites		Programming Scratch Maths	Data Handling Spreadsheets (online safety)		Programming Scratch-animated stories

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](http://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](http://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 (livestreams) 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](http://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 SEN PUPILS (Example that will be adapted according to pupil need)



### What I Must do to Keep Safe Online and With Devices



Online means anything connected to the internet. Most devices and



apps are connected to the internet.



Devices are technology like: computers, laptops, games consoles,



tablets and smart phones.



I will only use the devices I am allowed to use.



I will ask a trusted adult before I use new websites, games or apps.



I will ask for help if I'm stuck or not sure.





I will be kind and polite to everyone online.



I will tell a trusted adult if I feel worried, scared or nervous when I am using a device.



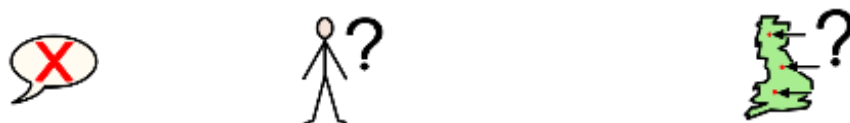
I will tell a trusted adult if I feel sad, angry or embarrassed when I am using a device.



I will tell a trusted adult if I feel bad or unsafe when I am using a device.



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 location.



I know that anything I do or say online might stay there forever.



It can be given to my family, my friends or strangers.



This could make me feel sad or embarrassed.



My trusted adults are \_\_\_\_\_ at school



My trusted adults are \_\_\_\_\_ at home



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 cyber-bullying?                                          |       |
| Are there any areas of online safety in which you would like training/further training? Please record them here. |       |

**Appendix G: online safety incident report log**

| Online safety incident report log |                               |                             |              |                                                           |
|-----------------------------------|-------------------------------|-----------------------------|--------------|-----------------------------------------------------------|
| Date                              | Where the incident took place | Description of the incident | Action taken | Name and signature of staff member recording the incident |
|                                   |                               |                             |              |                                                           |
|                                   |                               |                             |              |                                                           |
|                                   |                               |                             |              |                                                           |
|                                   |                               |                             |              |                                                           |
|                                   |                               |                             |              |                                                           |

## Appendix H

### Contact details for social networking sites

[The UK Safer Internet Centre](#) works with the social networking sites to disseminate their safety and reporting tools.

| Social networking site | Useful links                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ask.fm                 | <a href="#">Read Ask.fm's 'terms of service'</a><br><a href="#">Read Ask.fm's safety tips</a><br><b>Reporting on Ask.fm:</b><br>You do not need to be logged into the site (i.e. a user) to report.<br>When you move your mouse over any post on someone else's profile, you will see an option to like the post and also a drop down arrow which allows you to report the post. |
| BBM                    | <a href="#">Read BBM rules and safety</a>                                                                                                                                                                                                                                                                                                                                        |
| Facebook               | <a href="#">Read Facebook's rules</a><br><a href="#">Report to Facebook</a><br><a href="#">Facebook Safety Centre</a>                                                                                                                                                                                                                                                            |
| Instagram              | <a href="#">Read Instagram's rules</a><br><a href="#">Report to Instagram</a><br><a href="#">Instagram Safety Centre</a>                                                                                                                                                                                                                                                         |
| Kik Messenger          | <a href="#">Read Kik's rules</a><br><a href="#">Report to Kik</a><br><a href="#">Kik Help Centre</a>                                                                                                                                                                                                                                                                             |
| Snapchat               | <a href="#">Read Snapchat rules</a><br><a href="#">Report to Snapchat</a><br><a href="#">Read Snapchat's safety tips for parents</a>                                                                                                                                                                                                                                             |
| Tumblr                 | <a href="#">Read Tumblr's rules</a><br><a href="#">Report to Tumblr by email</a><br>If you email Tumblr take a screen shot as evidence and attach it to your email                                                                                                                                                                                                               |
| Twitter                | <a href="#">Read Twitter's rules</a><br><a href="#">Report to Twitter</a>                                                                                                                                                                                                                                                                                                        |
| Vine                   | <a href="#">Read Vine's rules</a><br><a href="#">Contacting Vine and reporting</a>                                                                                                                                                                                                                                                                                               |
| YouTube                | <a href="#">Read YouTube's rules</a><br><a href="#">Report to YouTube</a><br><a href="#">YouTube Safety Centre</a>                                                                                                                                                                                                                                                               |