

# Jubilee Online Safety Policy



## Contents

### 1. Introduction and Overview

- Rationale and Scope
- Roles and responsibilities
- How the policy be communicated to staff/pupils/community
- Handling complaints

### 2. Education and Curriculum

- Pupil Online Safety curriculum
- Staff and governor training
- Parent awareness and training

### 3. Expected Conduct and Incident Management

### 4. Managing the IT Infrastructure

- Passwords policy
- School website

### 5. Equipment and Digital Content

- Personal mobile phones and devices
- Digital images and video

### Review and Monitoring

## Scope

*This policy applies to all members of Jubilee Primary School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of the school Computing systems, both in and out of Jubilee Primary School.*

*The Education and Inspections Act 2006 empowers Headteachers / Principals to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties 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 / academy, 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 (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.*

*Jubilee will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents of incidents of inappropriate Online safety behaviour that take place out of school.*

## 1. Introduction and Overview

### Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Jubilee Primary School with respect to the use of IT-based technologies.
- safeguard and protect the children and staff of Jubilee Primary School.
- assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as online bullying which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

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

### Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence),
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites

- content validation: how to check authenticity and accuracy of online content

**Contact**

- grooming
- online bullying in all forms
- identity theft (including ‘frape’ (hacking Facebook profiles)) and sharing passwords

**Conduct**

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- extremism
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

(Ref Ofsted 2013)

Role	Key responsibility
Headteacher  Jo Eade / Tom Prestwich	To take overall responsibility for Online Safety provision <ul style="list-style-type: none"> <li>● To take overall responsibility for data and data security</li> <li>● To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements - LGfL</li> <li>● To be responsible for ensuring that staff receive suitable training to carry out their Online safety roles and to train other colleagues, as relevant</li> <li>● To be aware of procedures to be followed in the event of a serious e-safety incident.</li> <li>● To receive regular monitoring reports from the Online Safety Co-ordinator / Officer</li> <li>● To ensure that there is a system in place to monitor and support staff who carry out internal Online safety procedures( e.g. network manager)</li> </ul>
Designated Child Protection Lead/Online Safety co-ordinator  Alastair Crockett	Takes day to day responsibility for Online safety issues and has a leading role in establishing and reviewing the school Online safety policies / documents <ul style="list-style-type: none"> <li>● Promotes an awareness and commitment to Online safeguarding throughout the school community</li> <li>● Ensures that Online safety education is embedded across the curriculum</li> <li>● Liaises with school Computing technical staff</li> </ul>

	<ul style="list-style-type: none"> <li>● To communicate regularly with SLT and the designated Online safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs</li> <li>● To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident</li> <li>● To ensure that an Online safety incident log is kept up to date</li> <li>● Facilitates training and advice for all staff</li> <li>● Liaises with the Local Authority and relevant agencies</li> <li>● Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: <ul style="list-style-type: none"> <li>I. Sharing of personal data</li> <li>II. Access to illegal / inappropriate materials</li> <li>III. Inappropriate on-line contact with adults / strangers</li> <li>IV. Potential or actual incidents of grooming</li> <li>V. Online bullying and use of social media</li> </ul> </li> </ul>
Governors / Online safety governor	<p>To ensure that the school follows all current Online safety advice to keep the children and staff safe</p> <ul style="list-style-type: none"> <li>● To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub 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</li> <li>● To support the school in encouraging parents and the wider community to become engaged in e-safety activities</li> <li>● The role of the Online Safety Governor will include: <ul style="list-style-type: none"> <li>● regular review with the Online Safety Coordinator / Officer ( Including Online safety incident logs, filtering / change control logs )</li> </ul> </li> </ul>
Network Manager  Strictly Eduction	<p>To report any online safety related issues that arise, to the Online safety coordinator.</p> <ul style="list-style-type: none"> <li>● To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed</li> <li>● To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date)</li> <li>● To ensure the security of the school IT system</li> <li>● To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices</li> <li>● the school's policy on web filtering is applied and updated on a regular basis</li> <li>● LGfL is informed of issues relating to the filtering applied by the Grid</li> <li>● that he / she keeps up to date with the school's Online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as needed</li> <li>● that the use of the network / Virtual Learning Environment (LEARNING PLATFORM) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinator / Officer / Headteacher for investigation / action / sanction</li> <li>● To ensure appropriate backup procedures exist so that critical</li> </ul>

	<p>information and systems can be recovered in the event of a disaster.</p> <ul style="list-style-type: none"> <li>● To keep up-to-date documentation of the school's online security and technical procedures</li> </ul>
Teachers and all staff	<p>To embed online safety issues in all aspects of the curriculum and other school activities</p> <ul style="list-style-type: none"> <li>● To supervise and guide pupils carefully when engaged in learning activities involving online technology ( including, extra-curricular</li> <li>● To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws</li> </ul> <p>To read, understand and help promote the school's e-safety policies and guidance</p> <ul style="list-style-type: none"> <li>● To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy</li> <li>● To be aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices</li> <li>● To report any suspected misuse or problem to the online safety coordinator</li> <li>● To maintain an awareness of current online safety issues and guidance e.g. through CPD</li> <li>● To model safe, responsible and professional behaviours in their own use of technology</li> <li>● To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.</li> </ul>
Pupils	<p>Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (NB: at KS1 it would be expected that parents / carers would sign on behalf of the pupils)</p> <ul style="list-style-type: none"> <li>● have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations</li> <li>● to understand the importance of reporting abuse, misuse or access to inappropriate materials</li> <li>● to know what action to take if they or someone they know feels worried or vulnerable when using online technology.</li> <li>● to know and understand school policy on the use of mobile phones, digital cameras and hand held devices.</li> <li>● To know and understand school policy on the taking / use of images and on cyber-bullying.</li> <li>● To 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</li> <li>● To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home</li> </ul>

	<ul style="list-style-type: none"> <li>● to help the school in the creation/ review of e-safety policies</li> </ul>
Parents and Carers	<ul style="list-style-type: none"> <li>● To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images</li> <li>● To read, understand and promote the school Pupil Acceptable Use Agreement with their children</li> <li>● to access the school website / bug club / on-line student / pupil records in accordance with the relevant school Acceptable Use Agreement.</li> <li>● to consult with the school if they have any concerns about their children's use of technology</li> </ul>

**Communication:**

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

- Policy to be posted on the school websites
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

**Handling complaints:**

- 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 and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  - I. interview/counselling by tutor / Phase Leader / Online Safety Coordinator / Headteacher;
  - II. informing parents or carers;
  - III. removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system];
  - IV. referral to LA / Police.
- Our Online Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of online 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

## 2. Education and Curriculum

### Pupil Online safety curriculum

This school

- Has a clear, progressive Online safety education programme as part of the Computing curriculum / PSHE curriculum (See Jubilee Computing policy for more details). It is built on LA / LGfL online safeguarding and online literacy framework for EYFS to Y6/ national guidance. This covers a range of skills and behaviour appropriate to their age and experience, including:

- to STOP and THINK before they CLICK
  - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
  - 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 how to narrow down or refine a search;
  - In KS2 to understand how search engines work and to understand that this affects the results they see at the top of the listings;
  - to understand acceptable 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, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
  - 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;
  - To understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
  - To know how to report any abuse including online bullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
  - Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign.

- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- 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 respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying online; online gaming / gambling;

### **Staff and governor training**

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on online safety issues and the school's online safety education program.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and policies.

### **Parent awareness and training**

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
  - ✓ Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of online safe behaviour are made clear
  - ✓ Information leaflets; in school newsletters; on the school web site;
  - ✓ demonstrations, practical sessions held at school;
  - ✓ suggestions for safe Internet use at home;
  - ✓ provision of information about national support sites for parents.

## **3. Expected Conduct and Incident management**

Expected conduct

In this school, all users:

- ✓ are responsible for using the school Computing systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (at KS1 it would be expected that parents/carers would sign on behalf of the pupils.)
- ✓ need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- ✓ need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- ✓ 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
- ✓ will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking / use of images and on online bullying.

#### **Staff**

- ✓ are responsible for reading the school's Online safety policy and using the school Computing systems accordingly, including the use of mobile phones, and handheld devices.

devices.

#### **Students/Pupils**

- ✓ should have a good understanding of research skills and the need to avoid plagiarism
- ✓ and uphold copyright regulations

#### **Parents/Carers**

- ✓ should provide consent for pupils to use the Internet, as well as other technologies, as part of the Online safety acceptable use agreement form at time of their child's entry to the school
- ✓ should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

#### **Incident Management**

In this school:

- I. There is strict monitoring and application of the Online safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- II. All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- III. Support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with online safety issues
- IV. Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA
- V. Parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- VI. We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

#### **4. Managing the IT and Computing infrastructure**

##### **● Internet access, security (virus protection) and filtering**

This school:

Ensures that all pupils are closely supervised at all times when accessing information online or using the school's computers or iPads.

Uses the LGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only.

Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;

Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network.

Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns.

Requires staff to preview websites before use; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search.

Is vigilant when conducting 'raw' image search with pupils e.g. Google image search.

##### **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

##### **School website**

- I. The assistant head teacher/ computing lead takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained
- II. Uploading of information is restricted to our website authorisers: Currently the computing co-ordinator
- III. The school web site complies with the statutory DfE guidelines for publications
- IV. Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status
- V. The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. office@Jubilee.lambeth.sch.uk. Home information or individual e-mail identities will not be published;
- VI. Photographs published on the web do not have full names attached, we do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

## Pupil iPads

30 iPads are kept for the use of children. Only the assistant head teacher / computing lead is able to purchase and download apps on these iPads and their use by pupils is closely monitored at all times during lesson time. The computing lead ensures that all Apps installed are suitable and appropriate for the children using them and teachers are required to supervise children closely when using the iPads and especially when they are being used to access online content.

## 5. Equipment and Digital Content Personal mobile phones and mobile devices

- I. See our separate mobile phone policy. Staff use of personal devices
- II. Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- III. Staff will use a school phone where contact with students, parents or carers is required.
- IV. Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- V. If a member of staff breaches the school policy then disciplinary action may be taken.
- VI. Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

## Digital images and video In this school:

- I. 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;
- II. We do not identify pupils in online photographic materials
- III. Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- IV. If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- V. The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- VI. Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their IT scheme of work;

Date	28/11/2017
Approved by computing lead	
Approved by Head teacher	
Approved by governors	
Review date	28/11/2017