St John's Highbury Vale C of E Primary School
E-Safety Policy

1 Aims and objectives

1.1 This is an amended version of the 2011 London Grid for Learning (LGfL) Policy.

The Internet is an essential resource to support teaching and learning. The curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning, phones and touch screen tablet devices. Computer skills are vital to access life-long learning and employment; indeed Computing is now seen as an essential life-skill.

Young people have access to the Internet from many places, home, school, friends' homes, libraries and mobile devices. Schools have a number of services to help ensure that curriculum use is safe and appropriate, however access out of school does not usually have these services and has a range of risks associated with its use. Schools are ideally placed to help young people learn to become e-safe. This policy is designed to ensure safe Internet use by pupils and staff both in and outside school.

1.2 The aims of this eSafety policy are:

- To set out the key principles expected of all members of the school community at St John's with respect to the use of ICT-based technologies;
- To safeguard and protect the children and staff of St John's;
- To assist staff working with children to work safely and responsibly with ICT;
- To set clear expectations of behaviour relevant to responsible use of the internet;
- To have clear structures to deal with online abuse such as cyberbullying, which are cross referenced with other school policies;
- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where necessary, disciplinary action may be taken.

1.3 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
- content validation: how to check the authenticity of online content

Contact

- grooming
- cyber bulling
- identity theft and password sharing

Conduct

- privacy issues, including disclosure of personal information

- digital footprint and online reputation
- health and well-being, e.g. the amount of time spent online or gaming
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images)
- copyright, e.g. little care for intellectual property and ownership such as music, film and photographs

This policy applies to all members of St John's community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of St John's.

1.4 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 disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other eSafety incidents covered by this policy, which may take place outside St John's, 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.

St John's 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 eSafety behaviour that take place out of school.

1.5 Communication:
This policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website
- Policy to be part of school induction pack for new staff
- Acceptable use agreements to be issued to children and families when starting at St John's. Agreements will be issued again when children enter Key Stage 2.
- All staff to sign acceptable use agreements.
- Acceptable use agreements to be held on file in school.

1.6 Handling complaints:

- St John's will take all reasonable precautions to ensure eSafety, however 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. Pupil sanctions will be in line with the school behaviour policy.
- The eSafety Coordinator or Head Teacher act as first points of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of cyberbullying 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.

- Any incident that indicates that evidence of indecent images or offences concerning child protection may be contained on school computers should be referred immediately to the LADO (Local Authority Designated Officer), which may be referred to the Police.

2. Education and Curriculum

2.1 Pupil eSafety curriculum

St John's:

Has a clear eSafety education programme as part of the Computing curriculum. It is built on the LGfL (London Grid for Learning) e-Safeguarding and e-literacy framework for EYFS to Y6. This covers a range of skills and behaviours appropriate to children's age and experience, including:

- to Stop and Think before you Click;
- to discriminate between fact, fiction and opinion online;
- 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 refine a search;
- to understand acceptable behaviour when using ICT;
- to understand that 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 personal information online;
- to understand why they must not post pictures or videos of others without their permission;
- to know not to download files, e.g. music files, without permission;
- to have strategies for dealing with receipt of inappropriate materials;
- to create safe and secure passwords;
- to identify secure websites;
- to know the different types of malware that can affect a computer;
- to understand the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying;
- to know how to report any abuse including cyberbullying;
- to seek help if they experience problems when using ICT.

2.2 Staff training

St John's:

- Makes regular training available to staff on eSafety issues and the school's eSafety education programme through staff meetings and LBI/healthy schools training;
- Provides, as part of the induction process, all new staff with information and guidance on the eSafety policy and the school's Acceptable Use Agreement.

2.3 Parent awareness and training

St John's:

Provides advice, guidance and training for parents, including:

- Information leaflets: in school newsletters; via the school web site;

- distribution of ‘think u know’ for parents materials;
- suggestions for safe Internet use at home;
- provision of information about national support sites for parents.

3. Expected Conduct and Incident management

3.1 Expected conduct

At St John’s, all users of ICT:

- are responsible for using the school ICT 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);
- should 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 eSafety practice when using digital technologies, realise that the ESafety Policy covers their actions out of school, if related to their membership of the school;
- should understand the school policy on the use of mobile and digital devices.

3.2 Staff

- are responsible for reading the school’s eSafety policy and using the school ICT systems, mobile devices and mobile phones accordingly.

3.3 Parents/Carers

- should provide consent for pupils to use the Internet and other technologies as part of the eSafety acceptable use agreement at the time of their child’s entry to the school;
- should know and understand that the sanctions for misuse are in line with the school behaviour policy.

3.4 Incident Management

At St John’s:

- there is strict monitoring and application of the eSafety 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;
- 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;
- support is actively sought from other agencies as needed (eg the local authority, UK Safer Internet Centre helpline) in dealing with eSafety issues;
- monitoring and reporting of eSafety incidents takes place and contributes to developments in policy and practice in eSafety within the school;

- parents/carers are specifically informed of eSafety incidents involving young people for whom they are responsible, depending on the severity of the incident;
- We will contact the LADO if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- Any eSafety incidents will be dealt with in line with the behavior policy, staff code of conduct and policy on allegations of abuse against staff and volunteers.

4. Managing the ICT infrastructure

4.1 Internet access, security (virus protection) and filtering

St John's:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL 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 are logged and only available to staff with the approved 'web filtering management' status;
- Ensures network health through use of Sophos anti-virus software (from LGfL) and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes;
- 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;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age/subject appropriate web sites;
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; eg google junior
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;

- Informs staff and students that that they must report any failure of the filtering systems directly to the teacher /ICT Coordinator/Headteacher responsible for URL filtering;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and 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 and the LA.

4.2 Network management (user access, backup)

To ensure the network is used safely, St John's:

- Uses individual, audited log-ins for all users - the London USO system;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Has additional local network auditing software installed;
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Storage of all data within the school will conform to the UK data protection requirements;
- Ensures staff read and sign that they have understood the school's eSafety Policy. Online access to LGfL services is through a unique, audited username and password different username and password are used for access to our school's network;
- Staff access to the SIMs (School Information Management System) is controlled through a separate password for data security purposes;
- Provides pupils with an individual username and password for access to LGfL services and for other online services, e.g. Mathletics.
- Uses the London Grid for Learning's Unified Sign-On (USO) system for username and passwords;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- Provides staff with unique usernames and private passwords to access school systems. Staff and children are responsible for keeping their passwords private;
- Has set-up the network with a shared work area for pupils and one for staff;
- Requires all users always to 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;
- Has set-up the network so that users cannot download executable files / programmes;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date;

- Maintains equipment to ensure Health and Safety is followed
  e.g. projector filters cleaned by technician; equipment installed and checked by approved suppliers/LA electrical engineers;
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
  e.g. teachers access report writing module; SEN coordinator - SEN data;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school/LA approved systems;
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
  e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children;
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external audit's requirements;
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Follows Internet Service Provider (ISP) advice on Local Area and Wide Area security matters and firewalls. Routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security.
- Employs a part-time technician from a reputable organisation (Joskos) to monitor, maintain and support pupil/staff use of the school's ICT resources.

5. Email

St John's:

- Provides staff with an LGFL London Mail email account for their professional use and makes it clear that personal email should be through a separate account;
- Provides highly restricted (Safe mail) / simulated environments for e-mail with Key Stage 1 pupils and uses London Mail with older children as this has email content control;
- Does not publish personal e-mail addresses of pupils or staff on the school website;
- Will ensure that email accounts are maintained and up to date;
- Knows that spam, phishing and virus attachments can make emails dangerous. We use LGfL-provided technologies to help protect

users and systems in the school, including desktop anti-virus product Sophos;
- Has unique LGfL London Mail email addresses for all children, however has not issued them to children as yet.

6. Digital images and video

St John's:

- Obtains parental/carer permission for use of digital photographs or video as part of the school agreement form when a child joins the school;
- Does not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced videos/DVDs;
- Ensures staff sign the school's Acceptable Use Policy which includes a clause on the use of personal devices for taking pictures of pupils;
- Will obtain parental permission if specific pupil photos are used on the school web site or in other school publications;
- KS2 pupils are advised to be careful about placing personal photos on social network sites. They are taught to understand the need to maintain privacy settings so as not to make personal information public.
- KS2 pupils are taught that they should not post images or videos of others without their permission.

7. Photos and videos taken by parents/carers.

Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.

The parental letter concerning AUP's includes a paragraph concerning posting photos on social networking sites (see appendix 2)

Photos for personal use such as those taken by parents/carers are not subject to the Data Protection Act.

8. Mobile phones and other devices

-Student use of Mobile phones and digital device – (please see Use of Mobile Phones and Digital Devices Policy)

-Staff, Volunteers, Parents and Carers – (please see Use of Mobile Phones and Digital Devices Policy)

Date approved by the Curriculum and Achievement Committee: Jan 2015
Date approved by Governing Body: Approved Feb 2015
Date for next review: Autumn 2017

St John's HV School
eSafety Rules (KS1)

All pupils use computer facilities including internet access as an essential part of learning, as required by the National Curriculum. At Key Stage One parents/carers are asked to sign on behalf of their child to show that the eSafety Rules have been understood and agreed.

Child's name:

Parent's Consent for Web Publication of Work and Photographs
I agree that my child's work may be electronically published. We may also want to use videos or images of your child to illustrate some of our educational activities in and out of school.

Please tick the below If you agree for your child's images to be used for

- ☐ Internal school documents and displays
- ☐ School web site and school magazine
- ☐ Password protected class blog
- ☐ Within presentations to educational groups, including conferences, seminars etc.
- ☐ Portfolios of teachers' professional development

Parent's Consent for Internet Access
I have read and understood the school eSafety rules and give permission for my child to use ICT equipment and access the Internet at St John's.
I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.
I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	***Date:***
Please print name:	

Please complete, sign and return to the school office or class teacher

KS1 - Think before uou click

I will only use the Internet with permission from an adult.

I will only click on icons and links when I know they are safe

I will only send friendly and polite messages

If I see something I don't like on a screen, I will always tell an adult

My Name:

My Class:

Letter head

eSafety Rules (KS2)

All pupils use computer facilities including internet access as an essential part of learning, as required by the National Curriculum. Both pupils and parents/carers are asked to sign to show that the eSafety Rules have been understood and agreed.

Pupil name: ***Class:***

- I have read the rules and I understand the school eSafety Rules.
- I will use the computers, iPads, school network, mobile phones, internet and other technologies in a safe and responsible way at all times.
- I will only use the Internet when I have asked the teacher's permission.
- I know that network and Internet access may be monitored.

Signed: ***Date:***

Parent's Consent for Web Publication of Work and Photographs

I agree that my child's work may be electronically published. We may also want to use videos or images of your child to illustrate some of our educational activities in and out of school.

Please tick the below If you agree for your child's images to be used for

- ☐ Internal school documents and displays
- ☐ School web site and school magazine
- ☐ Password protected class blog
- ☐ Within presentations to educational groups, including conferences, seminars etc.
- ☐ Portfolios of teachers' professional development

Parent's Consent for Internet Access

I have read and understood the school eSafety rules and give permission for my child to use ICT equipment and access the Internet at St John's.
I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.
I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	***Date:***
Please print name:	

Please complete, sign and return to the school office or class teacher

St John's Highbury Vale Primary School

Rules for KS2 Children's Online Safety

1. I will always ask permission before using the internet or e-mail and only visit websites approved by my teacher.
2. I will not give out personal information about myself or other people such as my address, telephone number, parents' work address/telephone number. I will never send a person my picture or anything else without first checking with my parent/carer or teacher.
3. I will tell my teacher immediately if I come across any information that makes me feel uncomfortable (or a parent/carer if I am at home).
4. I will not open messages or files from people I do not know. They may contain malware or nasty messages and I will not reply to these. I will tell my parents or teacher immediately.
5. I will never arrange to meet someone I have ever only met on the internet or by e-mail, unless my parent or carer has given me permission and I take a responsible adult with me.
6. I will not bring computer files, memory sticks etc. into school without permission from my teacher. I will not open an attachment, download a file or install software or apps unless I have permission from my teacher.
7. I will never look at or delete anyone else's files without their permission.
8. I will be a good online citizen and not do anything that hurts other people or is against the law.