Computing & E-Safety Policy

Approved by Headteacher on: 29th October 2018

Review Date: Autumn Term 2020
INCLUSION STATEMENT

Barley Lane is a multicultural school where all children and adults are valued and respected as individuals, irrespective of:

- race
- religion
- belief
- gender
- ability
- disability
- social circumstances
- sexual orientation
- age
- part time contract or trade union memberships

The school is committed to safeguarding and promoting the welfare of children and the emotional wellbeing of staff so that every child and adult feels welcomed, fulfilled, safe, secure and confident.

Children and adults must be aware of their responsibility to report incidents of inappropriate behaviour.

School Aim
We aim for all pupils to:

Believe in themselves
Learn together
Persevere and
Succeed

And therefore be the best that they can be.

Contents

1. Introduction and Overview
   - Rationale and Scope
   - Roles and responsibilities
   - How the policy be communicated to staff/pupils/community
   - Handling complaints
   - Review and Monitoring

2. Education and Curriculum
   - Refer to additional guidance for teaching computing (APPENDIX 1)

3. Expected Conduct and Incident Management

4. Managing the ICT Infrastructure
   - Internet access, security (virus protection) and filtering
   - Network management (user access, backup, curriculum and admin)
   - Passwords policy
1. Introduction and Overview

Rationale and Scope
The purpose of this policy is to address both the curriculum and e-safety element of computing in Barley Lane Primary School. This policy will look to:

- set high expectations of the computing curriculum
- set out the key principles expected of all members of the school community at Barley Lane Primary School with respect to the use of ICT-based technologies inside and outside of the classroom
- safeguard and protect the children and staff of Barley Lane 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 cyberbullying 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 associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content
- Radicalisation.

**Contact**
- grooming
- cyber-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)
  Copyright (little care or consideration for intellectual property and ownership – such as music and film) (Ref Ofsted 2013).

This policy applies to all members of Barley Lane Primary School community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school’s ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers the Headteacher 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 e-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 published Behaviour Policy.

Barley Lane Primary 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 e-safety behaviour that take place out of school.

**Roles and Responsibilities**

<table>
<thead>
<tr>
<th>Executive Headteacher delegated to Associate Headteachers</th>
<th>To take overall responsibility for e-safety provision</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To take overall responsibility for data and data security (SIRO)</td>
</tr>
<tr>
<td></td>
<td>To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LGFL</td>
</tr>
<tr>
<td></td>
<td>To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant.</td>
</tr>
<tr>
<td></td>
<td>To be aware of procedures to be followed in the event of a serious e-</td>
</tr>
<tr>
<td>Safeguarding Lead / Designated Child Protection Lead</td>
<td>To receive regular monitoring reports from the Designated Safeguarding Lead (DSL) to ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (network manager)</td>
</tr>
<tr>
<td>Safeguarding Lead / Designated Child Protection Lead</td>
<td>Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school Information Technology policies</td>
</tr>
<tr>
<td>Safeguarding Lead / Designated Child Protection Lead</td>
<td>Promotes an awareness and commitment to e-safeguarding throughout the school community</td>
</tr>
<tr>
<td>Safeguarding Lead / Designated Child Protection Lead</td>
<td>Ensures that e-safety education is embedded across the curriculum</td>
</tr>
<tr>
<td>Safeguarding Lead / Designated Child Protection Lead</td>
<td>Liaises with school ICT technical staff</td>
</tr>
<tr>
<td>Safeguarding Lead / Designated Child Protection Lead</td>
<td>To communicate regularly with SLT and the designated e-safety Governor/committee to discuss current issues, review incidents</td>
</tr>
<tr>
<td>Safeguarding Lead / Designated Child Protection Lead</td>
<td>To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident</td>
</tr>
<tr>
<td>Safeguarding Lead / Designated Child Protection Lead</td>
<td>To ensure that an e-safety incident log is kept up to date</td>
</tr>
<tr>
<td>Safeguarding Lead / Designated Child Protection Lead</td>
<td>Liaises with the Local Authority and relevant agencies.</td>
</tr>
<tr>
<td>Safeguarding Lead / Designated Child Protection Lead</td>
<td>Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:</td>
</tr>
<tr>
<td>Safeguarding Lead / Designated Child Protection Lead</td>
<td>• sharing of personal data</td>
</tr>
<tr>
<td>Safeguarding Lead / Designated Child Protection Lead</td>
<td>• access to illegal / inappropriate materials</td>
</tr>
<tr>
<td>Safeguarding Lead / Designated Child Protection Lead</td>
<td>• inappropriate on-line contact with adults / strangers</td>
</tr>
<tr>
<td>Safeguarding Lead / Designated Child Protection Lead</td>
<td>• potential or actual incidents of grooming</td>
</tr>
<tr>
<td>Governors / E-safety governor</td>
<td>To communicate regularly with SLT and the designated e-safety Governor/committee to discuss current issues, review incidents</td>
</tr>
<tr>
<td>Governors / E-safety governor</td>
<td>To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident</td>
</tr>
<tr>
<td>Governors / E-safety governor</td>
<td>To ensure that an e-safety incident log is kept up to date</td>
</tr>
<tr>
<td>Governors / E-safety governor</td>
<td>To facilitate and ensure that teachers are promoting a use of e-safety when children are using technology</td>
</tr>
<tr>
<td>Governors / E-safety governor</td>
<td>To liaise with the DSL regularly.</td>
</tr>
</tbody>
</table>
| Network Manager/ Technician And LGFL Nominated contacts | • To report any e-safety related issues that arise, to the DSL 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  
• To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date.  
• To ensure the security of the school ICT system  
• To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices  
• the school’s policy on web filtering is applied and updated on a regular basis  
• LGFL is informed of issues relating to the filtering applied by the Grid  
• To ensure that he/she keeps up to date with the school’s e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant  
• To ensure that the use of the network/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the DSL /Headteacher for investigation/action/sanction  
• To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster  
• To keep up-to-date documentation of the school’s e-security and technical procedures  
• To ensure all LGFL related services are managed on behalf of the school including maintaining LGFL USO database of users and accounts. |
| Learning Platform Leader | • To ensure that all data held on pupils on the LEARNING PLATFORM is adequately protected. |
| Data Manager | • To ensure that all data held on pupils on the school MIS network have appropriate access controls in place |
| Teachers | • To embed e-safety issues in all aspects of the curriculum and other school activities  
• To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)  
• To ensure that pupils are fully aware of legal issues relating to electronic content such as copyright laws  
• To regularly promote a use of computing within their planning with the resources that are available  
• To use wider resources in their planning which will encourage creative and exciting lessons  
• Monitoring the way that ICT is taught on a regular basis  
• To support colleagues in the teaching of computing and the cross curricular use of technology  
• To ensure that children use computing equipment responsibly. |
| All staff | • To read, understand and help promote the school’s e-safety policies and guidance  
• To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy  
• To be aware of e-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 |
| To report any suspected misuse or problem to the e-safety coordinator  |
| To maintain an awareness of current e-safety issues and guidance e.g. through CPD |
| To model safe, responsible and professional behaviours in their own use of technology |
| 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. |

<table>
<thead>
<tr>
<th>Pupils</th>
</tr>
</thead>
<tbody>
<tr>
<td>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)</td>
</tr>
<tr>
<td>To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations</td>
</tr>
<tr>
<td>To understand the importance of reporting abuse, misuse or access to inappropriate materials</td>
</tr>
<tr>
<td>To know what action to take if they or someone they know feels worried or vulnerable when using online technology.</td>
</tr>
<tr>
<td>To know and understand school policy on the use of mobile phones, digital cameras and hand held devices</td>
</tr>
<tr>
<td>To know and understand school policy on the taking / use of images and on cyber-bullying.</td>
</tr>
<tr>
<td>To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school’s E-Safety Policy covers their actions out of school, if related to their membership of the school</td>
</tr>
<tr>
<td>To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home</td>
</tr>
<tr>
<td>To know and understand school policy on the use of mobile phones, digital cameras and hand held devices</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Extended Schools lead</th>
</tr>
</thead>
<tbody>
<tr>
<td>Educating Parents and raising awareness as instructed by Headteacher and Governors.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parents/ carers</th>
</tr>
</thead>
<tbody>
<tr>
<td>To support the school in promoting e-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</td>
</tr>
<tr>
<td>To read, understand and promote the school Pupil Acceptable Use Agreement with their children</td>
</tr>
<tr>
<td>To access the school website/LEARNING PLATFORM/on-line student/pupil records in accordance with the relevant school Acceptable Use Agreement</td>
</tr>
<tr>
<td>To consult with the school if they have any concerns about their children’s use of technology.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>External groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any external individual/organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school.</td>
</tr>
</tbody>
</table>

**Communication**

Responsibility of Computing Lead to ensure that the 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
Policy to be read by all members of 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
‘School staff Acceptable Use Agreement/Policy’ to be signed by all members of staff that have access to technology within the school.

Handling Complaints
The school will take all reasonable precautions to ensure e-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:
- Interview by Designated Safeguarding Lead informing parents or carers
- Removal of Internet or computer access for a period
- 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
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.

Review and Monitoring
The e-safety policy is referenced from within other school policies: Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education policies.

- The school has a DSL who will be responsible for document ownership, review and updates
- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- This computing curriculum and e-safety policy has been written by the Computing Lead and Network Manager and and updated and overseen by the designated Safeguarding Lead in accordance with statutory guidelines
- The Network Manager, designated Safeguarding Lead and Designated Computing Lead to regularly liaise to keep in line with the national requirements
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders. All amendments to the school e-safety policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum
- Refer to additional guidance for teaching computing (APPENDIX 1)

3. Expected Conduct and Incident management

Expected conduct
In this school, all users:
- 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.)
- 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 e-safety practice when using digital technologies out of school and realise that the school’s E-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 cyber-bullying.

**Staff**
- are responsible for reading the school’s e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

**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 e-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:
- there is strict monitoring and application of the e-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
- 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 (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues
- monitoring and reporting of e 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 / LSCB
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible
- 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 ICT infrastructure

Internet Access, Security (Virus Protection) and Filtering

This school:

- has the educational filtered secure broadband connectivity through the LGFL and so connects to the ‘private’ National Education Network;
- 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 available to staff with the approved ‘web filtering management’ status;
- uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- ensures network healthy through use of Panda endpoint anti-virus software 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/ Internet Literacy lessons;
- has blocked pupil and staff 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;
- ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- ensures pupils only publish within an appropriately secure environment: the school’s learning environment/ the London LEARNING PLATFORM/LGFL secure platforms such as J2Bloggy, etc.
- requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school’s website 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; e.g. yahoo for kids or ask for kids, Google Safesearchkids, …..
- never allows ‘raw’ image search with pupils e.g. Google image search;
- informs all users that Internet use is monitored;
- informs staff and students that they must report any failure of the filtering systems directly to the IT Staff who will if necessary escalates as to the LGFL Helpdesk
- 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 programmes;
- 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.
Network Management (user access, backup)

This school

- 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
- uses Impero ‘remote’ management control tools for controlling workstations/ viewing users/setting-up applications and Internet web sites, where useful
- has additional local network auditing software installed (spice works)
- ensures the 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, including new GDPR guidelines from May 2018
- pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- ensures staff read and sign that they have understood the school’s e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also provide a different username and password for access to our school’s network
- staff access to the schools' management information system is controlled through a separate password for data security purposes
- we provide pupils with an individual network log-in username. From Year 3 they are also expected to use a personal password
- 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 as these have far less security restrictions and inappropriate use could damage files or the network
- 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
- requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day and we also automatically switch off all computers at 7pm via enforced group policy
- has set-up the network so that users cannot download executable files and programmes
- has blocked access to music/media download or shopping sites – except those approved for educational purposes
- scans all mobile equipment with anti-virus/spyware (Panda End Point) before it is connected to the network
- 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 and the school provides them with a solution to do so
• makes clear that staff are responsible for ensuring that any computer, laptop and iPads loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs
• makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Intranet; finance system, Personnel system etc
• maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by ICT Staff, equipment installed and checked by approved Suppliers and LA approved 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
• ensures that access to the school’s network resources from remote locations by staff is restricted and access is only through schools network. E.g. teachers access their area/a staff shared area for planning documentation via remote logon
• 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 and MIS Support
• provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password (their USO username and password)
• 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 ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network
• our wireless network has been secured to industry standard Enterprise security level 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.

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 for access into our MIS system
• We require staff to change their passwords into the school systems, MIS, LGfL USO admin site, every 90 days.
**E-mail**
This school Provides staff with an email account for their professional use, schools e-mail address and makes clear personal emails are blocked.

- Does not publish personal e-mail addresses of staff on the school website. We use anonymous or group e-mail addresses, for example admin@Barleylane.Redbridge.sch.uk/headteacher@Barleylane.redbridge.sch.uk for communication with the wider public
- Will contact the Police if one of our staff or pupils receives or sends an e-mail that we consider is particularly disturbing or breaks the law
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police
- Knows that spam, phishing and virus attachments can make e-mails dangerous. We use a number of LGFL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Panda, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these, LGFL WebScreen2 filtering monitors and protects our Internet access to the World Wide Web.

Pupils:
- Year 5 and 6 Pupils are introduced to, and use e-mail as part of the Computing scheme of work
- Pupils are taught about the safety and ‘netiquette’ of using e-mail at home i.e. they are taught:
  - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher parent/carer
  - that an e-mail is a form of publishing where the message should be clear, short and concise
  - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
  - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.
  - to ‘Stop and Think Before They Click’ and not open attachments unless sure the source is safe
  - that they should think carefully before sending any attachments
  - embedding adverts is not allowed
  - that they must immediately tell a teacher/responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature
  - not to respond to or send malicious or threatening messages
  - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying
  - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them
  - that forwarding ‘chain’ e-mail letters are not permitted
- Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail, social media and we explain how any inappropriate use will be dealt with.

Staff:
- Staff can only use the Schools e-mail systems on the school system
- Staff only use school e-mail systems for professional purposes
• Access in school to external personal e mail accounts are blocked
• Never use email to transfer staff or pupil personal data unless data is encrypted. We use secure, LA/DfE approved systems. These include: S2S (for school to school transfer)
• Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school ‘house-style’:
  o the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used
  o the sending of chain letters is not permitted
  o embedding adverts is not allowed
• All staff sign our school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School Website
• The Executive Head teacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained, uploading of information is restricted to our website authorisers
• The school web site complies with the statutory DfE guidelines for publications
• 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
• The point of contact on the web site is the school address, telephone number and we use a general email contact. Home information or individual e-mail identities will not be published
• 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
• We do not use embedded geo data in respect of stored images.

Social Networking
• Refer to the Social Networking Policy

Video Conferencing
This school only uses the LGFL/Vscene connected to the Janet supported services for video conferencing activity.

CCTV
We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (retained by the school for 28 days), without permission except where disclosed to the Police as part of a criminal investigation.

6. Data Security

Management Information System Access and Data Transfer

Strategic and Operational Practices
At this school:
• the Executive Headteacher is the Senior Information Risk Officer (SIRO)
• staff are clear who are the contact for school information
• we ensure staff know who to report any incidents where data protection may have been compromised
• all staff are DBS checked and records are held in one central record
• we ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
  o staff
  o governors
  o pupils
  o parents.

This makes clear staffs’ responsibilities with regard to data security, passwords and access.
• We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services
• We require that any Protected and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home
• School IT staff with access to setting-up usernames and passwords for email, network access is working within the approved system and follow the security processes required by those systems
• We ask staff to undertake at least annual housekeeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions
• Staff have secure area(s) on the network to store sensitive documents or photographs
• We require staff to log-out of systems when leaving their computer
• We use the DfE S2S site to securely transfer CTF pupil data files to other schools
• We use the Pan-London Admissions system (based on USO FX) to transfer admissions data
• Staff with access to the Admissions system also use LGFL OTP tag as an extra precaution
• We use LGFL’s USO FX to transfer other data to schools in London, such as references, reports of children
• We use the LGFL secure data transfer system, USO Auto Update, for creation of online user accounts for access to broadband services and the London content
• We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area
• All servers are in lockable locations and managed by DBS-checked staff
• We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data
• Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure
• Paper based sensitive information is shredded, using cross cut shredder/ collected by secure data disposal service.

For further details, please refer to the Data Protection Policy.
6. Equipment and Digital Content

Personal Mobile Phones and Mobile Devices

Mobile Phones:
- Mobile phones brought into school are entirely at the staff member, pupils’ or visitors’ own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Pupil mobile phones which are brought into school must be handed into the Admin office or children in Year 6 to their Class Teacher for the phone to be stored in a specific container and collected at end of school day.
- The recording, taking and sharing of images, video and audio on any mobile phone is not allowed. All mobile phone use is to be open to scrutiny and the Head teacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or pupil need to contact each other during the school day, they should do so only through the School Office. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the Executive Headteacher.
- All mobile phones and personally-owned devices will be handed in at reception should they be brought into school.

Please see the Mobile Phone & Camera Policy for further details.

Staff Use of Personal Devices:
- Staff handheld devices, including mobile phones and personal cameras must be noted in school – name, make & model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- 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.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- If a member of staff breaches the school policy, then disciplinary action may be taken.
- 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:

- 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
- we do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs
- 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
- if specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high profile publications the school will obtain individual parental permission for its long term use
- the school blocks access to social networking sites or newsgroups
- 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 ICT scheme of work
- pupils are taught that they are under age and cannot sign up for any social media sites.

Asset disposal

- All electrical equipment is disposed of securely. Please refer to the Health & Safety Policy.
APPENDIX 1

Additional Guidance for Teaching Computing

2. Education and Curriculum

Expectations of the Computing Curriculum at Barley Lane Primary School

Objectives

Early Years

It is imperative in the foundation stage that children are given a broad and play-based experience of ICT in a range of contexts which include outdoor play. Early years learning environments should feature ICT scenarios based on experience in the real world, such as in role play. Children gain confidence, control and language skills through opportunities to work on whiteboards or drive a remote-controlled toy. Outdoor exploration is an important aspect and can be supported by ICT toys such as metal detectors, controllable traffic lights and walkie talkies. Recording devices can support children to develop their communication skills. This is also a significant practise that will support children who have English as an additional language.

Key Stage 1

By KS1 pupils should be taught to:

- understand what algorithms are, how they are implemented as programs on to digital devices and that programs execute by following a sequence of instructions
- write and test simple programs
- understand the basic concept of coding
- use logical reasoning to predict the behaviour of simple programs
- organise, store and manipulate and retrieve data in a range of digital formats
- communicate safely and respectfully online, keeping personal information private and recognise common uses of information technology beyond school.

Key Stage 2

By the end of KS2 pupils should be taught to:

- design and write programs that accomplish specific goals, including controlling or simulating physical systems; solver problems by decomposing them in to smaller parts
- use sequence, selection and repetition in programs; work with variables and various forms of input and output; generate appropriate inputs and predicted outputs to test programs
- use logical reasoning to explain how a simple algorithm works and to detect and correct errors in algorithms and programs
- understand computing networks including the Internet; how they can provide multiple services such as the World-wide web; and the opportunities they offer for communication and collaboration
- describe how internet search engines find and store data; use search engines effectively; be discerning in evaluating digital content; respect individuals and intellectual property; use technology responsibly, securely and safely
select, use and combine a variety of software on a range of digital devices to accomplish given goals, including collecting, analysing, evaluating and presenting data and information.

All pupils should 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 at home or at school.

**Planning**
The scheme of work used by Barley Lane comes from Rising Stars published scheme. As the school continues to develop its resources and expertise to deliver the computing curriculum, ICT will continue to be taught in line with the national curriculum and will allow for clear progression. Computing will continue to be taught by a designated ICT PPA teacher on a bi-weekly basis. The school aims to offer opportunities to extend their learning in computing. Staff should aim to implement to use the school’s resources within their lessons and planning to encourage cross curricular activity within the classroom.

**Resources and Access**
The school acknowledges the need to continually maintain, update and develop its resources and to make progress towards consistent, compatible PC system by investing in resources that will effectively deliver the strands of the national curriculum and support the use of computing across the school. Teachers are required to inform the computing lead or Network manager of any faults as soon as they are noticed.

**Cross Curricular Links**
The contribution of computing to teaching in other computing areas is more significant than ever. Computing contributes to all areas of teaching and learning and the use of it should be encouraged. For example, the internet provides useful research for humanities subjects whereas computing can be used to support maths based around database work. Computing enables children to present their information and conclusions in the most presentable and appropriate way.

In English:
ICT is a major contributor to the teaching of English. Through the development of keyboard skills and the use of computers, children learn how to edit and revise text. They learn how to improve the presentation of their work by using desktop publishing software.

In Maths:
Many ICT activities build upon the mathematical skills of the children. Children use computing in mathematics to collect data, make predictions, analyse results and present information graphically. They also acquire measuring techniques involving positive and negative numbers and including decimal places.

SMSC and Citizenship:
Computing contributes to the teaching of SMCS and citizenship as children learn to work together in a collaborative manner. They develop a sense of global citizenship by using the Internet, email and social media. Through the discussion of moral issues related to electronic communication, children develop a view about the use and misuse and they also gain a knowledge and understanding of the interdependence of people around the world.
Pupil E-safety Curriculum

This school:

- has a clear, progressive e-safety education programme as part of the Computing curriculum, e-safeguarding and e-literacy framework for EYFS to Y6 national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:
  
  o to STOP and THINK before they CLICK
  o to develop a range of strategies to evaluate and verify information before accepting its accuracy;
  o to be aware that the author of a website/page may have a particular bias or purpose and to develop skills to recognise what that may be;
  o to know how to narrow down or refine a search;
  o [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
  o 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;
  o to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
  o to understand why online ‘friends’ may not be who they say they are and to understand why they should be careful in online environments;
  o 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;
  o to understand why they must not post pictures or videos of others without their permission;
  o to know not to download any files – such as music files - without permission;
  o to have strategies for dealing with receipt of inappropriate materials;
  o [for older pupils] to understand why and how some people will ‘groom’ young people for sexual reasons;
  o to understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
  o to know how to report any abuse including cyberbullying; 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 Child Line 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 pupils about their responsibilities through an end-user Acceptable Use Policy which every pupil will sign/will be displayed throughout the school/will be displayed when a pupil logs on to the school network
- 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 on-line; on-line 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 e-safety issues and the school’s e-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 guidance on the e-safeguarding policy and the school’s Acceptable Use 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 e-safety 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.
Acceptable Use Agreement:
All Staff, Volunteers and Governors Agreement Form

Covers use of all digital technologies in school: i.e. e-mail, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I will follow the separate e-safety policy (including mobile and handheld devices).
- I will only use the school’s digital technology resources and systems for professional purposes or for uses deemed ‘reasonable’ by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow ‘good practice’ advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else’s password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access e-mail / Internet / intranet / network or other school systems I have access to.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted in accordance with the school’s network information security policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the school approved e-mail system for any school business, including communication with parents. I will only enter into communication regarding appropriate school business.
- I will only use the school’s approved systems to communicate with pupils, and will only do so for teaching & learning purposes.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or any filtering breach or equipment failure to BLPS IT Staff. I will not download any software or resources from the Internet that can compromise the network or is not adequately licensed, or which might allow me to bypass filtering and security systems.
- I will check copyright and not publish or distribute any work, including images, music and videos, that is protected by copyright, without seeking the author’s permission.
• I will not connect any device (including USB flash drives) to the network that does not have up-to-date anti-virus software, and I will keep any ‘loaned’ equipment up-to-date, using the school’s anti-virus and other LGFL filtering systems.

• I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.

• I will only use school approved equipment for any storage, editing or transfer of digital images, videos and ensure I only save photographs and videos of children and staff on the school approved system.

• I will follow the school’s policy on use of mobile phones and other devices at school.

• I will ensure that any private social networking sites or blogs that I create or actively contribute to are not confused with my professional role.

• I will ensure, where used, that I know how to use any social networking sites / tools securely, so as not to compromise my professional role.

• I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities.

• I will only access school resources remotely (such as from home) using the schools secure remote connections and follow e-security protocols to interact with them.

• I will ensure any confidential data is not transported from one location to another on any USB device, and that I agree to follow the school’s guidance for using Office 365.

• I understand that data protection policy requires that any information seen by me with regard to staff or pupil information that is held within the school’s information management system will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

• I will alert the school’s child protection officer, appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.

• I will only use any other/LA system I have access to in accordance with its policies.

• I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff or child protection officer at the school.

• I understand that all Internet usage and network usage can be logged, and that this information can be made available to the Head on their request.

• Staff that have a teaching role only: I will embed the school’s e-safety, digital literacy curriculum into my teaching.
Acceptable Use Agreement Form: Staff, Volunteers, Governors

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others’ e-safeguarding and I undertake to be a ‘safe and responsible digital technologies user’.

I understand that it is my responsibility to ensure that I remain up-to-date and that I read and understand the school’s most recent e-safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature ...................................................... Date ..................................................

Full Name .......................................................... (printed)

Job Title / Role ..........................................................
Think before you click

S
I will only use the Internet and email with an adult.

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

F
I will only send friendly and polite messages. I will only add nice pictures and words to my pages.

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

My daughter / son name(s): _________________________________

Parent / guardian signature: __________________________

Date: ___/___/___
Child’s Name: ____________________________________________________________

Class: _________________________________________________________________

APPENDIX 3 – Key Stage 2

KS2 Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- In lessons, I will only use the school’s computers for schoolwork and homework.
- During Computing and Coding club I will use the computer’s responsibly and only when supervised by a member of staff.
- I will only edit or delete my own files and not look at, or change other people’s files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- Websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher or another responsible adult.

I have read and understand these rules and agree to them.

Signed: _______________________________ Date: __________________

Parent / guardian signature: _________________________________________

Date: ____/____/____