###

### **Lidget Green Primary School**

Online E Safety Guide

|  |  |
| --- | --- |
| Approved by the Governing Body on: | December 2020 |
| To be reviewed on: | December 2022 |
| Signed on behalf of the Governing Body: | C:\Users\Deirdre_2\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\OXW6W8L3\D Bailey Sig.JPG |

NB. This guidance will be retained for a period of 7 years from replacement.

Version 2 / Dated: December 2020

### **Scope of the Policy**

This policy applies to all members of the Lidget Green School community (including staff, pupils, volunteers, parents/carers and visitors) who have access to, and are users of, school digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose 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, 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.

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

## **Roles and Responsibilities**

7

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. Online Safety is considered to be an integral part of Safeguarding and the nominated Governor for Safeguarding (Deirdre Bailey) will discuss Online Safety as part of her meetings with the DSL team, including monitoring of Online Safety monitoring logs.

### **Headteacher and Senior Leaders**

* The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Designated Safeguarding Lead who is also the Online Safety Lead.
* The Headteacher will follow the school’s Safeguarding procedures in the event of a serious online safety allegation being made against a member of staff. In the event of the allegation being made against the Headteacher, the Chair of Governors, supported by the Online Safety Lead will follow the appropriate procedures.
* The Headteacher is responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
* The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
* The Headteacher and the Online Safety Lead will ensure that the managed service provider (Datacable) carries out all the online safety measures that would otherwise be the responsibility of the school technical staff
* The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

### **Online Safety Lead**

* takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
* ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
* provides training and advice for staff
* liaises with school technical staff
* receives reports of online safety incidents to inform future online safety developments,
* records Online Safety concerns about individual pupils on CPOMS
* meets regularly with Online Safety Governor to discuss current issues and review incident logs
* attends relevant meetings of Governors
* reports regularly to Senior Leadership Team

### **Network Manager/Technical staff**

Those with technical responsibilities are responsible for ensuring:

* that the school’s technical infrastructure is secure and is not open to misuse or malicious attack
* that the school meets required online safety technical requirements
* that users may only access the networks and devices through a properly enforced password protection policy
* the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
* that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
* that the use of the network, internet and other digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and; Online Safety Lead for investigation/action/sanction
* that monitoring software and systems are implemented and updated as agreed

### **Teaching and Support Staff (including supply staff who have access to our systems)**

Are responsible for ensuring that:

* they have an up to date awareness of online safety matters and of the current school online safety policy and practices
* they have read, understood and signed the staff Acceptable Use policy
* they report any suspected misuse or problem to the Headteacher or Online Safety Lead for investigation, action or sanction
* all digital communications with pupils and parents/carers should be on a professional level and only carried out using official school systems
* online safety issues are embedded in all aspects of the curriculum and other activities
* pupils understand and follow the Online Safety Policy and acceptable use policies
* pupils develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
* in lessons where internet use is planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

### **Pupils:**

* are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement
* must develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
* will be expected to know and understand policies on the use of mobile devices, digital cameras and similar devices. They should also know and understand policies on the taking/use of images and on online-bullying.
* 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

### **Parents/carers**

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents’ evenings, newsletters, letters, website, social media and ClassDojo. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

* digital and video images taken at school events
* access to parents’ sections of the website
* their children’s personal devices in the school

### **Education & Training – Staff/Volunteers**

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

* A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
* All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school’s online safety policy and acceptable use agreements
* *The Online Safety Lead will receive regular updates through attendance at external training events and by reviewing guidance documents published by relevant organisations.*
* *This online safety policy and its updates will be presented to and discussed by staff in staff meetings*
* *The Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.*

### **Education – Pupils**

Whilst regulation and technical solutions are very important, their use must be balanced by educating *pupils* to take a responsible approach. The education of *pupils* in online safety/digital literacy is therefore an essential part of the school’s online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

In planning their online safety curriculum we refer to:

* [DfE Teaching Online Safety in Schools](https://www.gov.uk/government/publications/teaching-online-safety-in-schools)
* [Education for a Connected Word Framework](https://www.gov.uk/government/publications/education-for-a-connected-world)

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

* A planned online safety curriculum is provided as part of Computing/PHSE/other lessons and will be regularly revisited
* Key online safety messages are reinforced as part of a planned programme of assemblies and pastoral activities
* Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.
* Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
* Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
* *Pupils are helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.*
* *Staff should act as good role models in their use of digital technologies, the internet and mobile devices*

*In lessons where internet use is planned, pupils should be guided to sites checked as suitable for their use and processes put in place for dealing with any unsuitable material that is found in internet searches.*

* *Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.*
* *It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.*

### Education – Parents/carers

Many parents and carers have a limited understanding of online safety risks and issues, but should be helped to play an essential role in the education of their children and in the monitoring/regulation of the children’s online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

* *Letters, newsletters, web site*
* *Parents consultation evenings*
* *High profile events e.g. Safer Internet Day*
* *Reference to relevant web sites/publications*

### **Training – Governors**

Governors should take part in online safety training/awareness sessions. This may be offered in a number of ways:

* Attendance at training provided by the Local Authority Governance Services
* Participation in school training or information sessions for staff or parents
* Information sent by the Online Safety Lead

### Technical – infrastructure/equipment, filtering and monitoring

If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school/academy, as suggested below.

The school will be responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements

* There will be regular reviews and audits of the safety and security of school technical systems
* Servers, wireless systems and cabling must be securely located and physical access restricted
* All users will have clearly defined access rights to school technical systems and devices.
* All users *(in Year 1 and above)* will be provided with a username and secure password by the Network Manager, Linda Ioanna *who will keep an up to date record of users and their usernames.* Users are responsible for the security of their username and password.
* The “master/administrator” passwords for the school systems, used by the Network Manager (or other person) must also be available to the *Headteacher/Principal* or other nominated senior leader and kept in a secure place (e.g. school safe)
* The Network Manager under the direction of the Headteacher is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
* Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. The Network Manager will deal with requests for filtering changes and will report any concerns about these requests to the Online Safety Lead or the Headteacher
* Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
* *The school has provided differentiated user-level filtering* for children, staff and senior leaders
* *School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.*
* *Users to report any actual/potential technical incident or security breach to the Network Manager / Online Safety Lead*
* Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.
* An agreed procedure is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems. This is managed by the Network Manager and overseen by the Online Safety Lead.
* *An agreed policy is in place*, outlined in the Acceptable Use Policy *regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on school devices that may be used out of school.*
* *An agreed policy is in place* outlined in the Acceptable Use Policy *that forbids staff from downloading executable files and installing programmes on school devices.*
* *An agreed policy is in place* outlined in the Acceptable Use Policy *regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Digital personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.*

### **Mobile Technologies**

Mobile technology devices may be school or personally owned and might include: smartphone, tablet, notebook, laptop or other technology that usually has the capability of utilising the school’s wireless network. The device then has access to the wider internet which may include the school’s learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school’s online safety education programme.

The school acceptable use agreements for staff, pupils and parents/carers give consideration to the use of mobile technologies

The school allows only school owned devices to connect to the school’s WiFi and Intranet (see Mobile Phone and Camera policy for further details of use of devices in school).

For use of photographs on our system, including on our web-site, and the procedures governing our use and storage of personal information, please see the GDPR policy and guidance.

Use of Mobile Equipment used by pupils at home

During school closures, the Government expect children to be able to access teaching and learning online. Many of our families do not have the appropriate equipment to do this and the school has therefore bought a number of Chromebook computers to help them. These will been loaned to families who have signed an agreement, with the expectation that they will be used to support children’s education.