****

**ONLINE SAFETY POLICY**

Lambs Lane recognises its responsibilities for safeguarding children online and giving them the skills to use technology safely.

This online safety policy will be reviewed by the Full Governing Board.

|  |  |
| --- | --- |
| **Review Date:** | **Changes Made:** |
| June 2020 | * Name of policy to Online Safety – references throughout related to online safety instead of e-safety * **1.1** removal of governor online safety committee * **1.2** addition of information related to DSL responsibility with reference to Keeping Children Safe in Education statutory guidance. * **1.3** removal of name – Alex Leaver * **1.4** reference to learning platform manager and ICT technician removed. Addition of SLT into who is responsible for ensuring safe use of equipment and use of school’s network. Addition of Google Classroom. * **1.6** reference to Keeping Children Safe in Education statutory guidance * **1.7** addition of statement about DPO * **3.2** change of wording surrounding children messaging externally. * **3.5** Parental permission for photos on Google Classroom. Storage of photos in office 365 rather than S:drive now. Addition of Governors to people who should sign the acceptable use agreement. * **4.2** Reference to password access to Google Classroom. * **4.6** direction to DPO policy for more information * **4.7**  Reference to CPOMs when recording incidents * Deleted appendix about Data Protection – in line with Wokingham online safety guidelines. Separate policy for data protection. * **Appendix 2** reference to outside agencies and the need for them to follow the same policy guidelines * **Appendix 5** wording changed in relation to schools responsibility to take action when inappropriate content is accessed * Minor formatting and grammar changes throughout * Staff acceptable use agreement – should not disclose password to anyone (rather than stating that they could disclose it to people with admin rights) |
| May 2021 | * No changes made |

**NEXT REVIEW DATE:** 2022

**APPROVED BY COMMITTEE:** Full Governing Body

**“Children and young people need to be empowered to keep themselves safe – this isn’t just about a top-down approach. Children will be children – pushing boundaries and taking risks. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim”.**

**Professor Tanya Byron**

At Lambs Lane School, we recognise the opportunities and the innovative learning tools that advances in technology provide. This is deemed central to our role of supporting the learning and development needs of children and young people. It is therefore considered vital that all school staff, pupils and parents have a clear and agreed understanding of the benefits and risks of such technology.

There is a huge amount of guidance and advice available to staff from different sources, including their unions, and this policy can only cover the key issues. It is the responsibility of all staff at the school to remain vigilant and raise any concerns regarding omissions to this policy or practice in school with the Computing Subject Leader or the Headteacher.

# Roles and Responsibilities

## Governors

Governors are responsible for the approval of the Online Safety Policy (including Acceptable Use Agreements), ensuring that it is implemented and reviewing its effectiveness. In fulfilling this responsibility the governing body will appoint an online safety governor. Governors will require/undertake the following regular activities:

* Meetings with staff responsible for online safety.
* Monitoring of logged online safety incidents.
* Reporting to relevant governor committees.
* Keeping up to date with school online safety matters.

## Headteacher

The Headteacher is responsible for ensuring the overall safety, including online safety, of members of the school community. The Designated Safeguarding Lead (DSL) holds a responsibility for online safety as part of their role (as noted in the 2019 Keeping Children Safe in Education statutory guidance). On a practical day to day basis, the Online Safety Co-ordinator will have particular duties relating to online safety. However, the Headteacher will ensure the following:

* Staff with online safety responsibilities receive suitable and regular training enabling them to carry out their online safety roles and to train other colleagues as necessary.
* The Senior Leadership Team (SLT) receives regular monitoring reports.
* There is a clear procedure to be followed in the event of a serious online safety allegation being made against a member of staff.

## Online Safety Co-ordinator

As noted above, the Designated Safeguarding Lead holds a responsibility for online safety as part of their role (as noted in the 2019 Keeping Children Safe in Education statutory guidance). The online safety Co-ordinator is appointed to assist the DSL in their duties. The online safety Co-ordinator has day to day responsibility for online safety issues, ensures that policies are put into practice and supports the DSL in establishing and reviewing the school Online Safety Policy and associated documents. The Online Safety Co-ordinator will also:

* Provide training and advice for staff and ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
* Provide materials and advice for integrating online safety within schemes of work and check that online safety is taught on a regular basis.
* Liaise with the school’s Designated Safeguarding Lead.
* Ensure that online safety incidents are reported and logged and used to inform future online safety developments.
* Report to the governors and meet with them as required.
* Report regularly to the SLT.

## Technical support and Network Manager

The SLT and school’s technical support provider are responsible for ensuring that all reasonable measures have been taken to protect the school’s network(s), ensure the appropriate and secure use of school equipment and protect school data and personal information. This will involve ensuring the following:

* The IT infrastructure is secure and protected from misuse or malicious attack.
* The school meets the online safety technical requirements outlined in any relevant local authority online safety policy/guidance.
* Users may only access the school’s network(s) through a properly enforced password protection policy, in which passwords are changed at least twice a year.
* The school’s filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
* Online safety technical information is kept up to date, applied as necessary and passed on to others where relevant.
* Use of the network and Google Classroom is regularly monitored and any misuse/ attempted misuse reported to the Online Safety Co-ordinator or SLT for investigation and action.
* Appropriate steps are taken to protect personal information and secure data on all devices and removable media.
* Provide secure access to the school network from home using VPN.

## Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

* They are familiar with current online safety matters and the school Online Safety Policy and practices.
* They have read and understood the school’s Staff Acceptable Use Policy and signed to indicate agreement.
* They report any suspected misuse or problem to the Online Safety Co-ordinator or Headteacher for investigation and action.
* Digital communications with pupils (e-mail/blogging) should be on a professional level and only carried out using approved school systems.
* Online safety issues are embedded in all aspects of the curriculum and other school activities.
* Pupils understand and follow the school’s Online Safety and Acceptable Use Policies.
* Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations in relation to their age.
* They monitor IT activity in lessons, extra-curricular and extended school activities.
* They are aware of online safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement school policies with regard to these devices.
* In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and there is awareness of the procedure for dealing with any unsuitable material that is found in internet searches.

## Designated Safeguarding Lead(DSL)/ Child Protection Officer (CPO)

The DSL/CPO holds the responsibility for online safety as part of their role (as noted in the 2019 Keeping Children Safe in Education statutory guidance). They should be trained in online safety issues and be aware of child protection matters that may arise from any of the following:

* Sharing or loss of personal data
* Access to illegal/inappropriate materials
* Inappropriate online contact with adults/strangers
* Potential or actual incidents of grooming
* Cyberbullying

## Data Protection Officer (DPO)

The DPO has a related role which is detailed in Data Protection policies and related documentation

# Reviewing, Reporting and Sanctions

## Review

* This policy will be reviewed and updated annually, or sooner if necessary.
* The school will audit IT provision to establish if the Online Safety Policy is adequate and that its implementation is effective.

## Acceptable Use Agreements

* All users of the school IT equipment will sign the appropriate Acceptable Use Agreement. This includes all staff, governors and pupils.
* Parents will be asked to sign to show agreement with and support for the school’s policy.
* All users will be expected to resign agreements if the policy is reviewed and changed.

[See *‘Appendix 5’* for further information]

## Reporting and logging

* The school has clear guidelines as to what should be done if inappropriate content is found when accessing the internet.
* All pupils and staff should be aware of these guidelines.

[See *‘Appendix 1 – Course of action if inappropriate content is found’* for further information]

## Complaints regarding internet use

* Any complaints relating to internet misuse should be made in accordance with the school’s existing complaints procedure.
* Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

## Sanctions

* Failure to comply with the requirements of this policy will be dealt in line with the school’s existing behaviour policy.
* The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. This would constitute a disciplinary matter in the case of staff.

# Communications & Communication Technologies

## Mobile phones and personal handheld devices

* Pupils will not be allowed to bring mobile phones to school unless prior arrangements are made with the school. Mobile phones must be handed in to the office at the beginning of the school day.
* Where mobile phones are allowed in school they may not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or images is forbidden.
* Pupils will not be allowed to bring in games devices, particularly those which allow ad hoc networks to be established.
* Teacher/parent contact should normally be by the main school telephone and not via a mobile device except where off-site activities dictate the use of a mobile phone.
* Parent helpers in school and staff must ensure that they do not send personal messages, either audio or text, during contact time with pupils. If an exceptional emergency arises, they should arrange temporary cover whilst they make a call.
* Staff, helper and visitor mobile devices may normally be switched off or on silent during the times that children are present.
* No device in any of the school buildings should contain any content that is inappropriate or illegal.
* Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

## E-mail and messaging

* Pupils and staff will be informed that the use of school e-mail or messaging accounts will be monitored.
* Staff may access personal web-based e-mail accounts from school but **must not** use these for communications with parents or pupils.
* Under no circumstances should users use e-mail to communicate material (either internally or externally), which is defamatory or obscene.
* Pupils may only use approved e-mail or message accounts on the school system.
* Pupils should immediately tell a staff member if they receive an offensive e-mail or message.
* Pupils should not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone via an e­mail or message.
* Pupils should not send e-mails to an external person or organisation – staff can do this on the children’s behalf if needed.
* Information of a sensitive nature should not be sent by unencrypted e-mail.

## Social networking

For the purpose of this policy, social networking is considered to be any digital media or medium that facilitates interaction, e.g. Facebook, Twitter, blogs, chat rooms, online gaming, YouTube, Skype, Second Life, etc.

* Staff have a perfect right to use social networking sites in their private life. In doing so they should ensure that public comments made on social networking sites are compatible with their role as a member of staff and that they show the highest standards of professional integrity.
* Staff should regularly review their privacy settings on any personal social media sites.
* Pupil use of social networking should conform to age restrictions and will not be allowed in school unless this is part of an educational activity and has been authorised by an appropriate member of staff.
* The use of social networking ‘tools’, e.g. blogs, wikis, messaging, etc., within the school learning environment is both acceptable and to be encouraged.

[See *‘Appendix 2 – Social Networking Guidance’* for further information]

## Internet usage

* Pupils and staff will be informed that internet access will be monitored.
* The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.
* Users must not create, download, upload, display or access knowingly, sites that contain pornography or other unsuitable material that might be deemed illegal, obscene or offensive.
* Unauthorised users must not attempt to disable or reconfigure any filtering, virus protection or similar.
* All pupils using the internet, and associated communication technologies, will be made aware of the school’s online safety guidelines.
* Pupils will receive guidance in responsible and safe use on a regular basis

## Digital and video images

**Parental permission**

* The school will ensure that appropriate written permissions are obtained for the taking and use of digital and video images of pupils. Such use includes the school website, social media; display material in and around the school or off site; the school prospectus or other printed promotional material; local/national press.
* If specific individual pupil photographs are to be used publicly, such as on the school website, in the prospectus or any other high-profile publication, then a check should be made with individual parents for this additional use.
* Unless specific parental permission has been obtained, pupils will not be identified by name in any title or commentary accompanying digital or video images that is in the public domain. The school will also ensure that pupil names are not used in any file names used to save images; or in tags when publishing online.
* Where parental permission has not been obtained, or it is known that a pupil should not be photographed or filmed, every reasonable effort should be made to ensure that a pupil’s image is not recorded.
* Photos of children should not be added to the Google Classroom without parental permission.

**Storage and deletion**

* All images of pupils will be securely stored in one central location on the school’s Office 365 account.
* Where memory cards, USB drives, CDs or cloud storage are used during the process of capture or transfer, this must only be for temporary storage until images can be uploaded to the secure central location. The images should then be deleted from the temporary storage location and care taken to ensure they are not still available, e.g. in a recycle bin.
* Images of pupils should normally be deleted once a pupil has left the school unless being kept as part of archived records.

**Recording of images**

* All staff, governors and pupils must sign the Acceptable Use Agreement.
* School digital devices should always be used to record images of pupils (subject to variations as noted below in ‘Use of staff personal devices’).
* All pupils appearing in images should be appropriately dressed.
* Pupils must not take, use, share, publish or distribute images of others without appropriate staff permission.
* Where images are taken using devices with a facility to store or transfer data to other locations (e.g. automatic copying to online ‘cloud’ storage) care must be taken that the location of images of pupils is clearly understood and in line with ICO (Information Commission’s Office) guidance.
* All digital devices capable of taking photographs and recording sound or video, whether belonging to the school or personal, may be subject to scrutiny if required.
* Where volunteers are supporting school staff, they should abide by the same rules as school staff as far as is reasonable.

**Use of staff personal devices**

It is recognised that the most straightforward approach is not to allow use of staff personally owned devices (e.g. staff smartphones, personally owned cameras) to record images. If there is a need to photograph children on or off site with a personally owned device, the following procedures must be followed:

* It is only acceptable to use personally owned devices if there are no school devices that can be used or a school device has malfunctioned.
* Images will be transferred to a secure location on the school’s system as soon as possible and the originals/any copies deleted.
* Such staff personal devices should be passcode protected.

**Use of parents and carers mobile and personal devices**

* All parents and carers must sign the Parent/Carer Acceptable Use Agreement
* Parents and carers visiting Lambs Lane School may not use personally owned devices (e.g. smartphones, cameras) to record images of pupils, the school site or pupils work unless permission is given by the Headteacher or Online Safety Co-ordinator. Please see the variations detailed below in ‘Parents taking photographs or video’.
* Parents and carers visiting Lambs Lane School are requested to turn devices off or on to silent before they leave Reception.

**Parents taking photographs or video**

Lambs Lane Primary School allows the recording of images at ‘public’ events (e.g. school performances, open assemblies) but the following should apply:

* Photographs should not be distributed beyond either the school or the immediate family and friends of the child’s family.
* Photographs should not be posted on an open internet site.
* Photographs taken in school should not be posted on a social networking page that is accessible to the general public.

**Events/Activities involving multiple schools**

* When taking part in events organised by other schools or organisations, e.g. sports or music events, the schools involved will consider what image guidelines should apply.
* For larger events it is reasonable to expect that specific image guidelines should be in place. Where relevant these should include reference to press images.
* Those attending the event will be informed of the image guidelines that apply, e.g. a letter before the event, announcement at the event, or information in any printed programme.
* Although the school will make reasonable efforts to safeguard the digital images of pupils, parents should be made aware that at some types of event it is not always realistic to strictly enforce image guidelines. The school cannot therefore be held accountable for the use of images taken by parents or members of the public at events.

## School website

* The school website should include the school address, school e-mail, telephone and fax number including any emergency contact details.
* The school website should be used to provide information and guidance to parents concerning online safety policies and practice.
* Staff or pupils' home information should not be published.
* The copyright of all material posted must be held by the school or be clearly attributed to the owner where permission to reproduce has been obtained or given e.g. via Creative Commons licensing.

# Infrastructure and Security

## Security

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that procedures outlined within this policy are implemented by those responsible.

* SLT or IT technical support may monitor and record the activity of users on the school IT systems and users will be made aware of this.
* Servers, and communications cabinets should be securely located and physical access restricted.
* Wireless systems should be appropriately secured.
* All users will have clearly defined access rights to school IT systems. Details of the access rights available to groups of users will be accessible to SLT and IT technical support.
* Access to the school IT systems will cease when a pupil leaves or, in the case of a member of staff, ceases to be employed by the school.
* The ‘Administrator’ passwords for the school IT system, used by the IT Technical support are also available to the Computing and Online Safety coordinator and must be stored securely in school.

## Passwords

All staff have individual passwords. Pupils have a class password for accessing the network in school and individual passwords for accessing their Google Classroom. All users will have an individual log on to secure areas of the website or school social media sites.

Clear guidelines will be provided for all users which explain how effective passwords should be chosen. Further expectations of users are detailed below:

* No individual should tell another individual their password.
* No individual should log on using another individual’s password, unless they are a member of staff logging on as a pupil.
* Once a computer has been used, users must remember to log off so that others cannot access their information.
* Users leaving a computer temporarily should lock the screen (Windows key + L).
* Passwords should be changed at regular intervals.
* In the event that a password becomes insecure then it should be changed immediately.

[See *‘Appendix 3 – Password guidance’* for further information]

## Filtering

The school maintains and supports the managed filtering service provided by RM, the Internet Service Provider (ISP), and the South East Grid for Learning (SEGfL).

* Changes to network filtering should be approved by the Computing coordinator, Headteacher and the ICT technical support.
* Any filtering issues should be reported immediately to the ISP and/or SEGfL.

## Virus protection

* All computer systems, including staff laptops/devices, should be protected by an antivirus product which is preferably administered centrally and automatically updated.
* The antivirus product should allow for on-access scanning of files which may be being transferred between computers or downloaded from the internet. In the latter case, only dependable sources should be used.
* Staff should have access to and be able to use security software to remove adware and malware.

## Staff laptops/devices and flash drives

Staff laptops/devices are likely to be taken out of school and may well contain sensitive data (see Section 3.6). All staff laptops are encrypted. If staff need to use a flash drive, they should only use them if they are encrypted.

The following security measures should also be taken with staff laptop/devices:

* Laptops/devices must be out of view and preferably locked away overnight whether at school or home.
* Laptops/devices should never be left in a parked car, even in the boot.
* Screensavers should be set to lock after a maximum of 15 minutes.
* Laptops/devices should not be used for purposes beyond that associated with the work of the school, e.g. by the family of a member of staff.
* Where others are to use the laptop, they should log on as a separate user without administrator privileges.

[See *‘Appendix 5 – Acceptable Use Agreements’* for further information]

## Personal and sensitive data

* All users are responsible for only accessing, altering and deleting their own personal files. They must not access, alter or delete files of another user without permission.
* Sensitive data is any data which links a pupil’s name to a particular item of information and/or the loss of which is liable to cause individuals damage and distress. Therefore, such data:
  + must be encrypted on laptops/devices and any other removable media;
  + should not be e-mailed between staff;
  + should be deleted from laptops/devices at the end of an academic year or earlier if no longer required.
* Staff should take care not to leave printed documents with sensitive information open to view, e.g. by not collecting them promptly from printers, or leaving such documents on open desks. Sensitive information should be held in lockable storage when office staff are not present.
* There must be clear procedures for the safe and secure disposal of any device that records data or images, e.g. computers, laptops, memory sticks, cameras, photocopiers, etc.

[See *‘Appendix 4 – Sensitive & Non-Sensitive Data’* for further information]

*See Data Protection Policy for specific guidance in relation to the security of personal data.*

## Electronic devices - search and deletion

Schools now have the power to search pupils for items ‘banned under the school rules’ and the power to ‘delete data’ stored on seized electronic devices. Pupils can be searched and devices can be removed and investigated if it is suspected that they have pornography or other unsuitable material that might be deemed illegal, obscene or offensive. Also, data should be searched for and confiscated if it is suspected that they have been involved in cyber-bullying.

* A senior member of staff should be present when conducting a search for items ‘banned under the school rules’.
* At least two members of staff must be present when conducting a search.
* Data will be deleted or kept as evidence depending on the incident.
* Any incidents will be added to individual pupil’s records on CPOMs.

## Loading/installing software

For the purpose of this policy, software relates to all programs, images or screensavers, which can be downloaded or installed from other media.

* Any software loaded onto the school system or individual computers and laptops/devices must be properly licensed and free from viruses.
* Only authorised persons, such as the IT technical support or Computing/ Online Safety Coordinator, may load software onto the school system or individual computers.
* Where staff are authorised to download software to their own laptops/devices they must ensure that this is consistent with their professional role and that they are satisfied that any downloaded images and video clips do not breach copyright.

## Backup and disaster recovery

The school will define and implement a backup regime which will enable recovery of key systems and data within a reasonable timeframe should a data loss occur. This regime should include:

* The use of a remote location for backup of key school information, either by daily physical removal in an encrypted format, or via a secure encrypted online backup system.
* No data should be stored on the C:drive of any computer as it is liable to be overwritten without notice during the process of ghosting the computers.
* Staff are responsible for backing up their own data on teacher laptops/devices and should utilise any system that may be enabled such as automated copying of files to the school Office 365 account.
* Backup methods should be regularly tested by renaming and then retrieving sample files from the backup.

The school should also define a whole school IT disaster recovery plan which would take effect when severe disturbance to the school’s IT infrastructure takes place, to enable key school systems to be quickly reinstated and prioritised, including who would be involved in this process and how it would be accomplished.

# Online Safety Education

## Learning and teaching for pupils

* Pupils should be encouraged to adopt safe and responsible use of IT, the internet and mobile devices both within and outside school.
* Pupils should be helped to understand the need for an Acceptable Use Policy and, depending on age, asked to sign to indicate agreement.
* Pupils should be taught to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
* Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
* Key online safety messages will be included within the curriculum and reinforced as part of a planned programme of assemblies and other appropriate opportunities.
* Rules for the use of computers should be displayed in all rooms and displayed next to fixed site computers.

## Staff training

* Staff will be kept up to date through regular online safety training.
* Staff should always act as good role models in their use of IT, the internet and mobile devices.

## Parental support

The support of, and partnership with, parents should be encouraged. This will include the following:

* Awareness of the school’s policies regarding online safety and internet use; and where appropriate being asked to sign to indicate agreement.
* Practical demonstrations and training
* Advice and guidance on areas such as:
  + filtering systems
  + educational and leisure activities
  + suggestions for safe internet use at home

**Appendix 1 – Course of action if inappropriate content is found**

* If inappropriate web content is found (i.e. that is pornographic, violent, sexist, racist or horrific) the user should:
  + Turn off the monitor or minimise the window. If using a laptop, the user could close the monitor lid.
  + Report the incident to the teacher or responsible adult.
* The teacher/responsible adult should:
  + Ensure the well-being of the pupil.
  + Note the details of the incident, especially the web page address that was unsuitable (without re-showing the page to the pupils).
  + Report the details of the incident to the Online Safety Co-ordinator or DSL/ headteacher. Teachers will use the schools safeguarding system (CPOMs) to log the incident.
* The Online Safety Co-ordinator or DSL/ headteacher will then:
  + Log the incident and take any appropriate action.
  + Where necessary report the incident to the Internet Service Provider (ISP) so that additional actions can be taken.

**Appendix 2 – Social networking guidelines**

**Staff conduct**

* Staff will always conduct themselves with the highest standards of professional integrity and be aware that how they as individuals are perceived in the virtual world may reflect on how the school is perceived.
* Staff should give careful consideration when posting personal information as to how this might be viewed by pupils and parents even when the postings are within a ‘private’ online space.

**Access to social networking sites**

* Personal social networking sites should never be accessed during timetabled lessons and not normally during school working hours.
* Staff may not use school equipment to access personal social networking sites.
* If the school chooses to make ‘official’ use of social networking sites this should only be by authorised individuals.

**Posting of images and/or video clips**

* Photographic images and/or movie clips of children at the school or past pupils, up to the age of 18, should never be posted.
* Photographic images and/or movie clips of school staff should not be posted unless specific consent has been obtained.

**Privacy**

* Staff should recognise that their existing lists of friends/contacts/followers may include people who are part of both their private and professional lives.
* Staff should never be ‘friends’ with children at the school or past pupils up to the age of 18.
* Staff should not create new links with parents simply because they teach their children.
* Profile settings should be regularly checked, and updated as necessary, to ensure that posted comments and images are not publicly accessible.
* Any changes to social networking sites and privacy settings should be clearly understood.

**Additional considerations**

* Outside agency staff (e.g. sports coaches, music tutors) should follow the same policy guidelines as school staff members.

**Appendix 3 – Password guidance**

This guidance is intended for those adults using school systems but is based on good practice and should also feature in the teaching of, and advice to, pupils.

* Passwords should have a ‘strength’ of at least 12 where a letter is 1 and a number or punctuation mark is 2. The choice of password ‘strength’ should be appropriate to the data being protected and the potential risks associated with that data being compromised.
* Passwords should avoid following a pattern or being predictable.
* Passwords must not be easily guessable by anyone and therefore should not include:
  + Names of family, friends, relations, pets etc.
  + Addresses or postcodes of same
  + Birthdays
  + Telephone numbers
  + Car registration numbers
  + Unadulterated whole words
* Try to use in a password:
  + A mixture of letters and numbers
  + Punctuation marks
  + At least 8 digits

**Appendix 4 – Sensitive & Non-sensitive data**

Sensitive data will include:

* SEN records such as IPPs and Annual Review records
* Mark sheets and assessments
* Reports and Open Evening comments
* Personal data stored on the school’s Management Information System (SIMS)
* Photographic or video material
* Name, address and contact information

Non-sensitive data thus includes:

* General teaching plans
* Curriculum materials
* General correspondence of a non-personal nature

**Appendix 5 – Acceptable Use Agreements**

Included are:

* Pupil Acceptable Use Agreements
* Parent/Carer Acceptable Use Agreement
* Laptop Acceptable Use Agreement
* Staff Acceptable Use Agreement

**Key Stage 2 Pupil Acceptable Use Agreement**

**For my own personal safety:**

* I understand that the school will monitor my use of computers and digital communications.
* I will not tell anyone my username or password
* I will not try to use any other person’s username and password.
* I will be aware of ‘stranger danger’, when I am communicating online.
* I will not give out any personal information (e.g. home address and telephone number) about myself or anyone else when online.
* I will not arrange to meet people offline that I have communicated with online.
* I will immediately report any unpleasant or inappropriate pictures, videos, messages or audio files when I see it online.

**Respecting everyone’s rights to use technology as a resource:**

* I understand that the school computers are for educational use and that I will not use them for personal use unless I have permission to do so.
* I will not use the school computers for online gaming or video broadcasting (e.g. YouTube), unless I have permission from a member of staff to do so.

**Acting as I expect others to act toward me:**

* I will respect others’ work and property and will not access, copy, remove or alter any other user’s files, without the owner’s knowledge and permission.
* I will be polite and responsible when I communicate with others online.
* I will not use strong, aggressive or inappropriate language towards others online.
* I will not take or distribute images of anyone.

**Keeping secure and safe when using technology in school:**

* I will only use approved e-mail or message accounts on the school system.
* I will not use my personal handheld/external devices (e.g. mobile phones, etc.) in school.
* I will not try to upload, download or access any inappropriate materials.
* I will immediately report any damage or faults involving equipment or software.
* I will not open any attachments to e-mails, unless given permission to do so.
* I will ask for permission before sending an e-mail to an external person/organisation.

**Using the internet for research or recreation:**

* When using the internet, I will check that the information that I access is accurate.
* I will ensure that I have permission to use the original work of others in my own work.
* Where work is protected by copyright, I will not try to download copies (e.g. music and videos).

**Taking responsibility for my actions, both in and out of school:**

* I understand that the school has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school.
* I understand that if I break these rules there will be a consequence. This may also include loss of access to the school network/internet.

I have read and understood this agreement and will follow the rules outlined.

|  |  |  |  |
| --- | --- | --- | --- |
| Name/ Signature: |  | Date: |  |

**Key Stage 1 Pupil Acceptable Use Agreement**

**For my own personal safety:**

* I will not tell anyone my username or password and will not use other people’s.
* I will not talk to strangers online.
* I know not to give out personal information like my address, birthday and telephone number.
* I know that I must tell an adult if I see something that upsets me, or I am unsure of.
* I will check if I can click on things I haven’t seen before.
* I will not use the school computers for online games unless I have been given permission.
* I will respect others’ work.
* I will be polite and responsible when I talk to others online.
* I will not take or share pictures of anyone without their permission.
* I will use computers responsibly at home.

I have read and understood this agreement and will follow the rules outlined.

|  |  |  |  |
| --- | --- | --- | --- |
| Name/ Signature: |  | Date: |  |

**Parent/Carer Acceptable Use Agreement**

The school seeks to ensure that *students/pupils* have good access to IT to enhance their learning and, in return, expects pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school’s work.

======================================================================================

**Acceptance of Use Form**

|  |  |
| --- | --- |
| Parent/Carer’s Name: |  |
| *Student/Pupil’s* Name: |  |

As the parent/carer of the above pupil, I understand that my son/daughter will have access to the internet and to IT systems at school.

I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of IT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and IT systems. I also understand that although internet filtering systems usually work very well, inappropriate content may occasionally still be accessible, but in this instance the school will take appropriate action with the service provider to request such content is removed.

I understand that my son’s/daughter’s activity on the IT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child’s online safety.

|  |  |
| --- | --- |
| Signature: |  |
| Date: |  |

**Laptop/Devices Acceptable Use Agreement**

1. **Introduction**

* This agreement applies to all laptops and other associated devices which are loaned to staff and therefore remain the property of the school.
* It should be read in conjunction with the school’s Online Safety Policy
* All recipients and users of these devices should read and sign the agreement.

1. **Security of equipment and data**

* The laptop and any other equipment provided should be stored and transported securely. Special care must be taken to protect the laptop and any removable media devices from loss, theft or damage. Users must be able to demonstrate that they took reasonable care to avoid damage or loss.
* Staff should understand the limitations of the school’s insurance cover.
* Government and school policies regarding appropriate use, data protection, information security, computer misuse and health and safety must be adhered to. It is the user’s responsibility to ensure that access to all sensitive information is controlled.

1. **Software**

* Any additional software loaded onto the laptop should be in connection with the work of the school. No personal software should be loaded.
* Only software for which the school has an appropriate licence may be loaded onto the laptop or device. Illegal reproduction of software is subject to civil damages and criminal penalties.
* Users should not attempt to make changes to the software and settings that might adversely affect its use.

1. **Faults**

* In the event of a problem with the laptop or iPad, the school’s IT Technician/Network Manager should be contacted.

**Declaration:**

I have read and understood the above and also the school’s Online Safety Policy and agree to abide by the rules and requirements outlined.

|  |  |
| --- | --- |
| Name: |  |
| Signature: |  |
| Date: |  |

|  |  |
| --- | --- |
| Laptop serial number: |  |
| IPad serial number: |  |

# Staff Acceptable Use Agreement

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school’s Online Safety policy for further information and clarification.

* I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner.
* I appreciate that IT includes a wide range of systems, including mobile phones, PDAs, digital cameras, e-mail, social networking and that IT use may also include personal ICT devices when used for school business.
* I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
* I understand that my use of school information systems, internet and e-mail may be monitored and recorded to ensure policy compliance.
* I will respect system security and I will not disclose any password or security information to anyone.
* I will not install any software or hardware unless authorised, e.g. on a school laptop.
* I will ensure that personal data, particularly that of pupils, is stored securely through encryption and password and is used appropriately, whether in school, taken off the school premises or accessed remotely in accordance with the school Online Safety policy.
* I will respect copyright and intellectual property rights.
* I will ensure that electronic communications with pupils (including e-mail, instant messaging and social networking) and any comments on the web (including websites, blogs and social networking) are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
* I will promote Online safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.
* I will ensure that pupil use of the internet is consistent with the school’s Online Safety Policy.
* When working with pupils, I will closely monitor and scrutinise what pupils are accessing on the internet including checking the history of pages when necessary.
* I will ensure that computer monitor screens are readily visible, to enable monitoring of what the children are accessing.
* I know what to do if offensive or inappropriate materials are found on screen or printer.
* I will report any incidents of concern regarding pupils’ safety to the appropriate person, e.g. Online Safety Co-ordinator and/or SLT member.

The school may exercise its right to monitor the use of the school’s information systems, including internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school’s information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sounds.

|  |  |
| --- | --- |
| Name: |  |
| Signature: |  |
| Date: |  |