# Online Safety Policy

Review February 2021

## Background and Rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even more true for children, who are generally much more open to developing technologies than many adults. In many areas technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on social and emotional development and learning
- Inappropriate use of social media

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

## Policy and leadership

This section begins with an outline of the key people responsible for developing our online safety policy and keeping everyone safe with ICT. It also outlines the core responsibilities of all users of ICT in our school. It goes on to explain how we maintain our policy and then to outline how we try to remain safe while using different aspects of ICT

## Responsibilities: ICT Leader

Our ICT Leader is the person responsible to the Principal and governors for the day to day issues relating to online safety. The online safety Leader:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies and documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- provides training and advice for staff
- attends relevant meetings and committees of Governing Body
- reports regularly to the Vice Principal (Lead DSL)
- Ensures the ICT Manager
    - liaises with The Elliot Foundation (TEF)
    - liaises with RM Support
    - receives reports of online safety incidents through Impero and generates half termly reports of incidents to inform future online safety developments
    - reports regularly to the Principal
    - receives appropriate training and support to fulfil their role effectively
    - has responsibility for blocking / unblocking internet sites in the school's filtering system / passing on requests for blocking / unblocking to the ICT Helpdesk
    - maintains external filtering services and ensures systems are effective (RM Safety Net and Impero)

**Responsibilities: Lead Safeguarding DSL (Vice Principal)**

- meets with online safety governor to discuss current issues, review incident logs on My Concern and filtering change control logs on Impero
- maintains logs of any occasions where the school has used its powers of search and deletion of electronic devices
- alongside the IT Manager, reviews monitoring logs on Impero and follows up on incidents in accordance with the following policies; Safeguarding, Behaviour and Acceptable Use.

**Responsibilities: Governors**

Our governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors receiving regular information about online safety incidents and monitoring reports. A member of the governing body has taken on the role of online safety governor which involves:

- regular meetings with the ICT Leader and/or Safeguarding Lead with an agenda based on:
    - monitoring of online safety incident logs
    - monitoring of filtering change control logs
    - monitoring logs of any occasions where the school has used its powers of search and deletion of electronic devices
    - reporting to relevant Governor's' committee/meeting

**Responsibilities: Principal**

- The Principal is responsible for ensuring the safety (including online safety) of members of the school community, although the day to day responsibility for online safety is delegated to the

ICT Leader.

- The Principal and Vice Principal will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

**Responsibilities: classroom based staff**

Teaching and Support Staff 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 school's Acceptable Use Policy for staff (Appx A)
- they report any suspected misuse or problem to the ICT Leader or ICT Manager
- they will report online safety incidents (eg cyberbullying) on My Concern
- digital communications with students (email / voice) will be on a professional level and only carried out using official school systems (eg. Google Classroom)
- online safety issues are embedded in the curriculum and other school activities.

Responsibilities: ICT Manager

The ICT Manager is responsible for ensuring that:

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- users may only access the school's networks through a properly enforced password protection policy
- shortcomings in the infrastructure are reported to the Principal or Vice Principal so that appropriate action may be taken.
- the school's monitoring and filtering system (Impero) is working on all school devices and logs are checked regularly.

**Policy development, monitoring and review**

This online safety policy has been developed by a working group made up of:

- ICT Leader
- ICT Manager
- Principal and Vice Principal
- Governors (especially the online safety governor)
- Pupils

**Schedule for development / monitoring / review of this policy**

| | |
|---|---|
| The implementation of this online safety policy will be monitored by the: | Safeguarding Governor<br>under the direction of the ICT Leader |

| | |
|---|---|
| Monitoring will take place at regular intervals: | Annually |
| The governing body will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals: | Annually |
| The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be: | February 2021 |
| Should serious online safety incidents take place, the following external persons / agencies should be informed: | The Elliot Foundation (TEF) |

**Policy Scope**

This policy applies to all members of the school community (including but not limited to staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Principals, 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 online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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.

**GDPR**

In order to be fully GDPR compliant, all online user accounts will be managed through the school MIS. Using an Identity Management service (RM Unify) all accounts can be monitored and managed by the IT Lead and Manager. This will ensure that;

- All staff and students that leave the school will have their accounts suspended
- All student accounts will be managed through one system
- All students and staff will be provided with individual accounts

**Acceptable Use Policies (Appx A)**

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign their consent before being given access to school systems. Record of consent can be found here.

Acceptable use policies are provided for:

- Pupils (EYFS + KS1 / KS2)

- Adults working with Young Children
- Parents / carers when accessing the school system

Acceptable use policies are revisited and resigned annually at the start of each school year and amended accordingly in the light of new developments and discussions with the children which take place at the time. Copies are sent home for further discussion with parents.

Staff and student teachers sign when they take up their role in school and in the future if significant changes are made to the policy. Students/volunteers/Dinner ladies

When a child enters the school, parents are requested to provide permission for whether their child's image (still or moving) and their child's work may be published within school and/or on the school website, school blog, facebook page or the school's twitter feed. If a parents/carers do not wish their child's image to be used then this preference is recorded on school records. A list of pupils whose image should not be published is produced and updated by Senior School Secretary. This list is made available to all staff.

Induction policies for all members of the school community include this guidance.

**Self-Evaluation**

Evaluation of online safety is an on-going process and links to other self-evaluation tools used in school in particular to pre Ofsted evaluations along the lines of the Self Evaluation Form (SEF). The views and opinions of all stakeholders (pupils, parents, teachers and governors) are taken into account as a part of this process.

**Whole School approach and links to other policies**

This policy has strong links to other school policies as follows:

<u>Core ICT Policies</u>

Online safety Policy: How we strive to ensure that all individuals in school stay safe while using ICT.

Mobile Phone Policy: Appropriate use of mobile phones in school
Social Media Guidelines: How to use Social Media when in a professional role.
Email - Good practice : Communicating guidelines within the workplace.
Acceptable Use Policies (Appx A) : How to use technology in an acceptable way.

<u>Other policies relating to safety</u>

Preventing and Tackling Bullying:

How our school strives to illuminate bullying – link to cyber bullying

PSHE:

online safety has links to this – staying safe

Safeguarding:

Safeguarding children electronically is an important aspect of online safety. The online safety policy forms a part of the school's safeguarding policy

Behaviour:

Linking to positive strategies for encouraging online safety and sanctions for disregarding it.

**Illegal or inappropriate activities and related sanctions**

The school believes that the activities listed below are inappropriate in a school context: **some are illegal**.

Users will not engage in these activities when using school equipment or systems (in or out of school). Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images (illegal - The Protection of Children Act 1978)
- grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)
- possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)
- criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Additionally the following activities are considered unacceptable on ICT kit provided by the school:

- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Birmingham Local Authority and / or the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- Online gambling and non-educational gaming
- Use of personal social networking sites / profiles for non-educational purposes

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

| Pupil Sanctions | Refer to class teacher | Refer to e-safety coordinator | Refer to Principal or Vice Principal | Refer to Police | Inform parents/ carers | Removal of network/ internet access | Warning | Further sanction e.g. detention/ exclusion |
|---|---|---|---|---|---|---|---|---|
| Deliberate accessing or trying to access material that could be considered illegal (see previous list) | √ | √ | √ | | √ | √ | √ | √ |
| Unauthorised use of non-educational sites during lessons | √ | | | | √ | √ | | |
| Unauthorised use of mobile phone/ digital camera/ other handheld device | √ | | √ | | √ | | | |
| Unauthorised use of social networking/ instant messaging/ personal email | √ | | √ | | √ | | | |
| Unauthorised downloading or uploading of files | √ | | | | | | √ | |
| Allowing others to access the school network, using the account of a member of staff | √ | √ | √ | | √ | √ | √ | |
| Attempting to access or accessing the school network, using another pupil's account | √ | √ | √ | | | √ | √ | |
| Attempting to access or accessing the school network, using the account of a member or staff | √ | √ | √ | | √ | √ | √ | |
| Corrupting or destroying the data of other users | √ | √ | √ | | √ | √ | √ | |
| Sending an email, text, or instant message that is regarded as offensive, harassment or of a bullying nature | √ | √ | √ | | √ | √ | √ | √ |
| Continued infringements of the above, following previous warnings or sanctions | √ | √ | √ | √ | √ | √ | √ | √ |
| Actions which could bring the school into disrepute or breath the integrity of the ethos of the school | √ | √ | √ | | √ | √ | √ | |
| Using proxy sites or other means to subvert the school's filtering system | √ | √ | √ | | √ | √ | √ | |
| Accidentally accessing offensive or pornographic material and flailing to report the incident | √ | √ | √ | | √ | | | |
| Deliberately accessing or trying to access offensive or pornographic material | √ | √ | √ | √ | √ | √ | √ | √ |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act. | √ | √ | √ | | √ | √ | √ | |

| Staff Sanctions | Refer to line manager | Refer to Principal or Vice Principal | Refer to Tefat | Refer to Police | Refer to Technical Support Staff for action re filtering etc | Warning | Suspension | Disciplinary action |
|---|---|---|---|---|---|---|---|---|
| Deliberate accessing or trying to access material that could be considered illegal (see previous list) | √ | √ | √ | √ | √ | √ | √ | √ |
| Excessive or inappropriate personal use of the internet/ social networking sites/ instant messaging/ personal email | √ | √ | | | √ | √ | | |
| Unauthorised downloading or uploading of files | √ | √ | | | √ | √ | | |
| Allowing others to access school network by sharing username and passwords or attempting to access/ accessing the school network, using another person's account | √ | √ | | | | √ | | |
| Careless use of personal data e.g holding or transferring data in an insecure manner | √ | √ | | | | √ | | |
| Deliberate actions to breach data protection or network security rules | √ | √ | | | √ | √ | √ | |
| Corrupting or destroying the data of other users causing deliberate damage to hardware or software | √ | √ | √ | | | √ | √ | √ |
| Sending an email, text, or instant message that is regarded as offensive, harassment or of a bullying nature | √ | √ | √ | | | √ | √ | |
| Using personal email/ social networking/ instant messaging/ text messaging to carry out digital communications with pupils | √ | √ | √ | | | √ | | |
| Actions which could compromise the staff member's professional standing | √ | √ | | | | √ | | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | √ | √ | √ | | | √ | √ | √ |
| Using proxy sites or other means to subvert the school's filtering system | √ | √ | | | √ | √ | √ | |
| Accidentally accessing offensive or pornographic material and flailing to report the incident | √ | √ | | | √ | √ | | |
| Deliberately accessing or trying to access offensive or pornographic material | √ | √ | √ | √ | √ | √ | √ | √ |
| Breaching copyright or licensing regulations | √ | √ | | | | √ | | |
| Continued infringements of the above, following previous warnings or sanctions | √ | √ | √ | | | √ | √ | √ |

**Audit / Monitoring / Reporting / Review**

The Safeguarding Lead will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be reviewed by the Principal or Vice Principal and a governor on a half termly basis.

**Use of handheld technology (USB, personal phones and handheld devices)**

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- The use of USB sticks and external hard drives are not permitted in school unless approved by SLT and encrypted.
- Members of staff are permitted to bring their personal mobile devices into school. They are required to use these in accordance with the Mobile Phone Policy.

**Email**

Access to email is provided for all users in school via the intranet page accessible via the web browser from their desktop/chromebook/laptop.

These official school email services may be regarded as safe and secure and are monitored.

- Staff and pupils will use only the school email services to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored
- Pupils have access to an individual email account for communication within school.
- A structured education programme is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email.
- Staff may only access personal email accounts on school systems outside of teaching hours.
- Users must immediately report, to their class teacher / online safety coordinator – in accordance with the Safeguarding school policy the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

**Use of digital and video images**

- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they will recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images will only be captured using school equipment; the personal equipment of staff will not be used for such purposes.
- Care will be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.

**Use of web-based publication tools**

Our school uses the public facing website, http://www.billesleyschool.co.uk/ and the school's blog, facebook page and twitter feed for sharing information with the community beyond our school. This includes, from time-to-time celebrating work and achievements of children. All users are required to consider good practice when publishing content.

- Personal information will not be posted on the school website and only official email addresses

(provided as links rather than appearing directly on the site) will be used to identify members of staff (never pupils).

- Only pupil's first names are used on the website, and only then when necessary.
- Detailed calendars are not published on the school website.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
    - Pupils' full names will not be used anywhere on a website, blog, facebook or twitter and never in association with photographs
    - Photographs of pupils will not be published where parents/carers have requested that the school do not publish images of their child(ren).

**Professional standards for staff communication**

In all aspects of their work in our school teachers abide by the Teachers' Standards as described by the DfE https://www.gov.uk/government/publications/teachers-standards Teachers translate these standards appropriately for all matters relating to online safety.

Any digital communication between staff and pupils or parents / carers (email, chat, Google Classroom etc) must be professional in tone and content.

- These communications may only take place on official (monitored) school systems.
- Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice. The views and experiences of pupils are used to inform this process also.

**Filtering**

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a school buying broadband services from RM Education we automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the ICT Manager (with ultimate responsibility resting with the Principal or Vice Principal and governors). They manage the school filtering, in line with the processes outlined below and keep logs of changes to and breaches of the filtering system.

All users have a responsibility to report immediately to class teachers, ICT Leader, ICT Manager or another adult in school any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe will be blocked.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education / Training / Awareness

Pupils are made aware of the importance of filtering systems through the school's online safety education programme. Staff users will be made aware of the filtering systems through:

- signing the AUP (Appx A)
- briefing in staff meetings, training days, and further updates as necessary.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement (Appx A) and through online safety awareness sessions.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment.

Audit / reporting

Logs of filtering change controls and of filtering incidents are made available to

- The Principal
- The Elliot Foundation (TEF)

This filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

**Online Safety Education**

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 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. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

E- Safety education will be provided in the following ways:

- A planned online safety programme will be provided as part of ICT, PHSE and other lessons and will be regularly revisited – This is based on the DFE Teaching Online Safety in School guidance.
- We a wide range of resources including the use of CEOP's Think U Know site as a basis for our online safety education http://www.thinkuknow.co.uk/teachers/resources/ (Hector's World at KS1 and Cyber Café at KS2)
- Key online safety messages will be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
- Pupils will be helped to understand the need for the pupil AUP(Appx A) and encouraged to adopt safe and responsible use of ICT both within and outside school.
- In lessons where internet use is pre-planned, it is best practice that pupils will 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.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff will be vigilant in monitoring the content of the websites the young people visit.

**Information Literacy**

- Pupils will be taught in all lessons to be critically aware of the content they access online and be guided to validate the accuracy of information by employing techniques such as:
    - Checking the likely validity of the URL (web address)
    - Cross checking references (can they find the same information on other sites)
    - Checking the pedigree of the compilers / owners of the website
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are taught how to make best use of internet search engines to arrive at the information they require

**Staff training**

Staff receive regular 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. 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 online safety policy and acceptable use policies which are signed as part of their induction
- The ICT Leader and ICT Manager will receive regular updates through attendance at TEF or other information / training sessions and by reviewing guidance documents released by the DfE.
- The ICT Leader will provide advice, guidance and training as required to individuals as required on an ongoing basis.

**Parent and carer awareness raising**

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's online experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

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

- Letters, newsletters, web site, Youtube account, social media
- Parents evenings and parent workshops

**Wider school community understanding**

The school will offer family learning courses in ICT, media literacy and online safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e safety will also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

**Appendix A: Acceptable Use Policies**

The following pages contain the Billesley Primary School Acceptable Use Policies:

- Acceptable Use Policy for Learners in EYFS.
- Acceptable Use Policy for Learners in KS1.
- Acceptable Use Policy for Learners in KS2.
- Acceptable Use Policy for Adults Working with Young People.
- Acceptable Use Policy for Our Schools and Trustees.
- Acceptable Use Policy for Community Users.
- Acceptable Use Policy for Pupils and Parents

# Acceptable use policy agreement – Pupil (EYFS)

I want to feel safe all the time. I agree that I will:

- I will only use activities that an adult says are OK.
- I will take care of the computer and other equipment.
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will tell an adult if I see something that upsets me on the screen.
- only work with people I know in real life
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- never agree to meet a stranger
- I know that if I break the rules I might not be allowed to use a computer.

I understand these computer rules and will do my best to keep them.

| Class: | Date: |
|---|---|
| My name: | |

# Acceptable use policy agreement – Pupil (KS1)

I want to feel safe all the time. I agree that I will:

- always keep my passwords secret
- I will only use activities that an adult says are OK.
- I will take care of the computer and other equipment.
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will tell an adult if I see something that upsets me on the screen.
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- only work with people I know in real life
- make sure all messages I send are polite
- not give my mobile phone number to anyone who is not a friend in real life
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- not load photographs of myself onto the computer
- never agree to meet a stranger
- I know that if I break the rules I might not be allowed to use a computer.

I understand these computer rules and will do my best to keep them.

| Class: | Date: |
|---|---|
| My name: | |

# Acceptable use policy agreement – Pupil (KS2)

When I am using the computer or other technologies, I want to feel safe all the time. I agree that I will:

- always keep my passwords a secret
- I understand that my use of the internet will be monitored
- I will not try to access anything illegal.
- I will tell an adult if I find any damage or faults with technology, however this may have happened.
- only visit sites which are appropriate to my work at the time
- work in collaboration only with friends and I will deny access to others
- tell a responsible adult straight away if anything makes me feel scared or uncomfortable online
- make sure all messages I send are respectful
- show a responsible adult if I get a nasty message or get sent anything that makes me feel uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend
- only email people I know or those approved by a responsible adult
- only use email / cloud services which have been provided by school
- talk to a responsible adult before joining chat rooms or networking sites
- always keep my personal details private (my name, family information, journey to school, my pets and hobbies are all examples of personal details).
- always check with a responsible adult and my parents before I show photographs of myself
- never meet an online friend without taking a responsible adult that I know with me

**I know that once I post a message or an item on the internet then it is completely out of my control.**

I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow these guidelines:

| | | |
|---|---|---|
| Class: | | Date: |
| My Name: | | |

# Acceptable use policy agreement
# Adults working with Young People

INSPIRE our children to succeed
CREATE excitement for learning
ACHIEVE EXCELLENCE

This agreement is between:
**Billesley Primary School and** _____(Staff name)

Background
Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (laptops, email, social media, Google Drive etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school in the online safety policy.
- I will not disclose my username or password to anyone else, nor will I try to use anyone else's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.
- I will install 2-Step Verification for Google onto my account. (Speak to J.Stamp/K.Rogerson)

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

The school and the Elliot Foundation Academy Trust have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will only use my personal mobile ICT devices as agreed in the Online Safety and Mobile Phone Policy and then in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not use personal email addresses on the school ICT systems except in an emergency
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that all of my data is stored using Google Drive
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- Where personal data is transferred outside the secure school network, it must be encrypted using USB storage device.
- I understand that our Confidentiality Statement requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened and understand that I may be liable to charges.

When using the internet in my professional capacity or for sanctioned personal use:

- 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 download or distribute copies (including music and videos).
- I understand that I am responsible for my actions in and out of school:
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school (see Social Media Policy.)
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could involve a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the policy.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines.

| | |
|---|---|
| Name: | |
| Signed: | |
| Role: | |
| Date: | |

# Acceptable use policy agreement Governors

INSPIRE our children to succeed
CREATE excitement for learning
ACHIEVE EXCELLENCE

This agreement is between:

**Billesley Primary School and** _____(Name)

This policy aims to ensure that any communications technology (including computers, mobile devices/phones etc.) is used to supporting learning without creating unnecessary risk to users. Governors will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- learners are made aware of risks and processes for safe digital use
- all adults and learners have received the appropriate acceptable use policies and any required training
- the school has appointed an Online Safety Lead and a named Trustee takes responsibility for Online Safety
- an Online Safety Policy has been written by the school
- the Online Safety Policy and its implementation will be reviewed annually
- the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright laws are not breached
- learners are taught to evaluate digital materials appropriately x parents are aware of the acceptable use policy
- parents will be informed that all technology usage may be subject to monitoring, including website addresses and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit use of technology to establish if the Online Safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff

I confirm that I have read, understood and will adhere to the above.

Name: _____

Signature: _____

Date: _____

# Acceptable use policy agreement
# Community Users

INSPIRE our children to succeed
CREATE excitement for learning
ACHIEVE EXCELLENCE

This agreement is between:
**Billesley Primary School and** _____(Name)

This policy aims to ensure that community users of school digital technologies will be responsible users and stay safe while using these systems and devices. The policy is intended to protect school systems, devices and users from accidental or deliberate misuse that could put the security of the systems and users at risk.

I understand that:

- I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school.
- I understand that my use of school systems and devices and digital communications will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or that may cause harm or distress to others.
- I will not try to use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident; I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programs of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- 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 download or distribute copies (including music and videos).

I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices and other technology access.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name _____ Signature _____

Date_____

INSPIRE our children to succeed
CREATE excitement for learning
ACHIEVE EXCELLENCE

## Pupil Acceptable Use Policy

This is the Pupil Acceptable Use Policy for our school. The purpose of this policy is to promote positive and responsible computer and online behaviour. Please read it carefully.

- I will only use the school Internet and network for my school work or when a teacher has given permission.
- I will only use my school email address / school cloud services in school.
- I will make sure that all messages I sent are polite and respectful.
- I will be careful when opening emails from people I don't know and I will ask an adult if I'm unsure whether to open it.
- I will not share my passwords. • I will not look at or delete other people's work or files.
- I will make sure all my contact with other people at school is responsible. I will not bully pupils or teachers online.
- I won't look for or look at unpleasant or rude web sites. I will check with a teacher if I think a website might be unsuitable.
- I will not reply to any nasty messages or anything which makes me feel uncomfortable, and will instead show my teacher.
- I won't give out my personal details, such as my name, address, school or phone number on the Internet. I will not meet people I've met on the Internet (unless I have told my parents and they come with me). I will never agree to meet a stranger.
- I won't upload or download any pictures, writing or movies which might upset people.
- I won't try to install software onto the school network because it might have a virus.
- I will be careful with keyboards, mice, headphones and all other equipment, and when turning a computer on or off.
- I know that once I post an item on the internet then it is completely out of my control.
- I will try to follow these rules all the time because I know they are designed to keep me safe.
- If I'm not sure about anything, I will ask a teacher for advice.
- I understand that everything I do on the computers at school is monitored and anything I do on a computer may be seen by someone else.
- I know that the school can talk to my parents if a teacher is worried about my online safety

INSPIRE our children to succeed
CREATE excitement for learning
ACHIEVE EXCELLENCE

## Parent Acceptable Use Policy

- I have read and discussed my child's Acceptable Use Policy with them and I understand what is expected of them.
- I understand that the school has discussed the Acceptable Use Policy with my child and that they have received, and will continue to receive, ongoing online safety education to help them understand the importance of safe use of technology and the Internet – 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 emerging technology and the Internet.
- I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the Internet.
- I understand that the school will provide my child with a school email account / school cloud services account.
- I understand that my child's activity on the ICT 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 technology at home and will inform the school if I have concerns over my child's online safety.
- I will contact the school if my child makes comments or says things that concern me, or if their behaviour and things they are interested in change significantly.
- I will inform the school if my child sends or receives any communications (such as email, social media) that suggests identification with a particular group, cause or ideology.
- I agree to support and uphold the principles of this policy in relation to my child and their use of the Internet, at home and at school.
- I agree to support my child with interacting in school homework sites such as Bugclub, TT Rockstars and other sites recommended by the school.
- I agree to uphold the principles of this policy in relation to my own use of the Internet, when that use is related to the school, employees of the school and other students at the school.

Signed (Parent / Guardian)

_____ Date _____

Document