# On-line Safety Policy

## Date: March 2016

Signed

_____

## Next Review: March 2018

Bussage Primary School is a Church of England Voluntary Aided Primary School and this policy is written within the context of the Christian faith, practice and values which underpin our ethos, and which are in keeping with our Trust Deed

## Development / Monitoring / Review of this Policy

This On-line Safety policy has been developed by a working group made up of:

- *Head Teacher*
- *Coordinator*
- *Staff – including Teachers, Support Staff, Technical staff*
- *Governors*

## Schedule for Development / Monitoring / Review

| | |
|---|---|
| This On-line Safety policy was approved by the *Governing Body on:* | *Spring 2016* |
| The implementation of this On-line Safety policy will be monitored by the: | *SLT* |
| Monitoring will take place at regular intervals: | *Annually* |
| The *Governing Body via the Communications Committee* will receive a report on the implementation of the On-line Safety policy generated by the monitoring group (which will include anonymous details of On-line Safety incidents) at regular intervals: | *Annually* |
| The On-line 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 On-line Safety or incidents that have taken place. The next anticipated review date will be: | *Spring 2017* |
| Should serious On-line Safety incidents take place, the following persons should be informed: | *A. Ferguson (DSP)*<br>*D. Cockshull (backup DSP)* |

The school will monitor the impact of the policy using:

- *Logs of reported incidents*

# Scope of the Policy

This policy applies to all members of the *school* (including staff, children / children, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the *school*.

The Education and Inspections Act 2006 empowers Head Teachers to such extent as is reasonable, to regulate the behaviour of children 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 On-line Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

# Roles and Responsibilities

The following section outlines the On-line Safety roles and responsibilities of individuals and groups within the school:

## Governors:

*Governors* are responsible for the approval of the On-line Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about On-line Safety incidents and monitoring reports. A member of the *Governing Body* has taken on the role of *On-line Safety Governor*. The role of the On-line Safety *Governor* will include:

- regular meetings with the On-line Safety Co-ordinator
- regular monitoring of On-line Safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors

## Head Teacher and Senior Leaders:

- The *Head Teacher* has a duty of care for ensuring the safety (including On-line Safety) of members of the school community
- The Head Teacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious On-line Safety allegation being made against a member of staff.
- The Head Teacher and Senior Leaders are responsible for ensuring that the On-line Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their On-line Safety roles and to train other colleagues, as relevant.
- The Head Teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal On-line Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

## On-line Safety Coordinator (DSP):

- leads the On-line Safety committee
- takes day to day responsibility for On-line Safety issues and has a leading role in establishing and reviewing the school On-line Safety policies.
- ensures that all staff are aware of the procedures that need to be followed in the event of an On-line Safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of On-line Safety incidents and creates a log of incidents to inform future On-line Safety developments,
- meets regularly with On-line Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

# Network Manager / Technical staff:

The *Network Manager (Thomas Keble)* is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required On-line Safety technical requirements and any Local Authority / other relevant body On-line Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy (if it has one), is applied and updated on a regular basis
- that they keep up to date with On-line Safety technical information in order to effectively carry out their On-line Safety role and to inform and update others as relevant
- that the use of the network / internet / / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the On-line Safety Coordinator

# Teaching and Support Staff

are responsible for ensuring that:

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

# Child Protection / Safeguarding Designated Person

should be trained in On-line Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

## Children:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good On-line Safety practice when using digital technologies out of school and realise that the *school's* On-line Safety Policy covers their actions out of school, if related to their membership of the school

## Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local On-line Safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good On-line Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / blog
- their children's personal devices in the school (where this is allowed)

## Community Users

Community Users who access school systems / website as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school systems.

# Policy Statements

## Education – children

Whilst regulation and technical solutions are very important, their use must be balanced by educating children to take a responsible approach. The education of children in On-line Safety is therefore an essential part of the school's On-line Safety provision. Children and young people need the help and support of the school to recognise and avoid On-line Safety risks and build their resilience.

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

- A planned On-line Safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key On-line Safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Children should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- in lessons where internet use is pre-planned, it is best practice that children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where children are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, children may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

# Education – parents / carers

Many parents and carers have only a limited understanding of On-line Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, website,
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

# Education & Training – Staff / Volunteers

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

- A programme of formal On-line Safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff should receive On-line Safety training as part of their induction programme, ensuring that they fully understand the school On-line Safety policy and Acceptable Use Agreements.
- The On-line Safety Coordinator will receive regular updates through attendance at external training events (e.g. from LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This On-line Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The On-line Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

# Training – Governors

**Governors should take part in On-line Safety training / awareness sessions**, with particular importance for those who are members of any sub-committee / group involved in technology / On-line Safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation
- Participation in school training / information sessions for staff

# Technical – infrastructure / equipment, filtering and monitoring

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

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school / academy technical systems and devices.
- The Head Teacher is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

# Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and children need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not

covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other children / children in the digital / video images.

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that children / children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Children must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.
- Children' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of children / children are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers.

# Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

**The school must ensure that:**

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices

# Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

| | Staff & other adults | | | Children / Children | | | |
|---|---|---|---|---|---|---|---|
| **Communication Technologies** | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission |
| Mobile phones may be brought to school | ✓ | | | ✓ | | | |
| Use of mobile phones in lessons | | ✓ | | ✓ | | | |
| Use of mobile phones in social time | ✓ | | | ✓ | | | |
| Taking photos on mobile phones / cameras | | | ✓ | | | | ✓ |
| Use of other mobile devices eg tablets, gaming devices | | | ✓ | | | | ✓ |
| Use of personal email addresses in school, or on school network | | | ✓ | ✓ | | | |
| Use of school email for personal emails | | | ✓ | ✓ | | | |
| Use of messaging apps | | | ✓ | ✓ | | | |
| Use of social media | ✓ | | | ✓ | | | |
| Use of blogs (the school blogsite) | ✓ | | | | | | ✓ |

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and children should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and children / children or parents / carers (email) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses and passwords may be used at KS1, while student children at KS2 will be provided with individual school email addresses and passwords for educational use.
- Children should be taught about On-line Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

# Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for children and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to children, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to children, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and On-line Safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

# Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

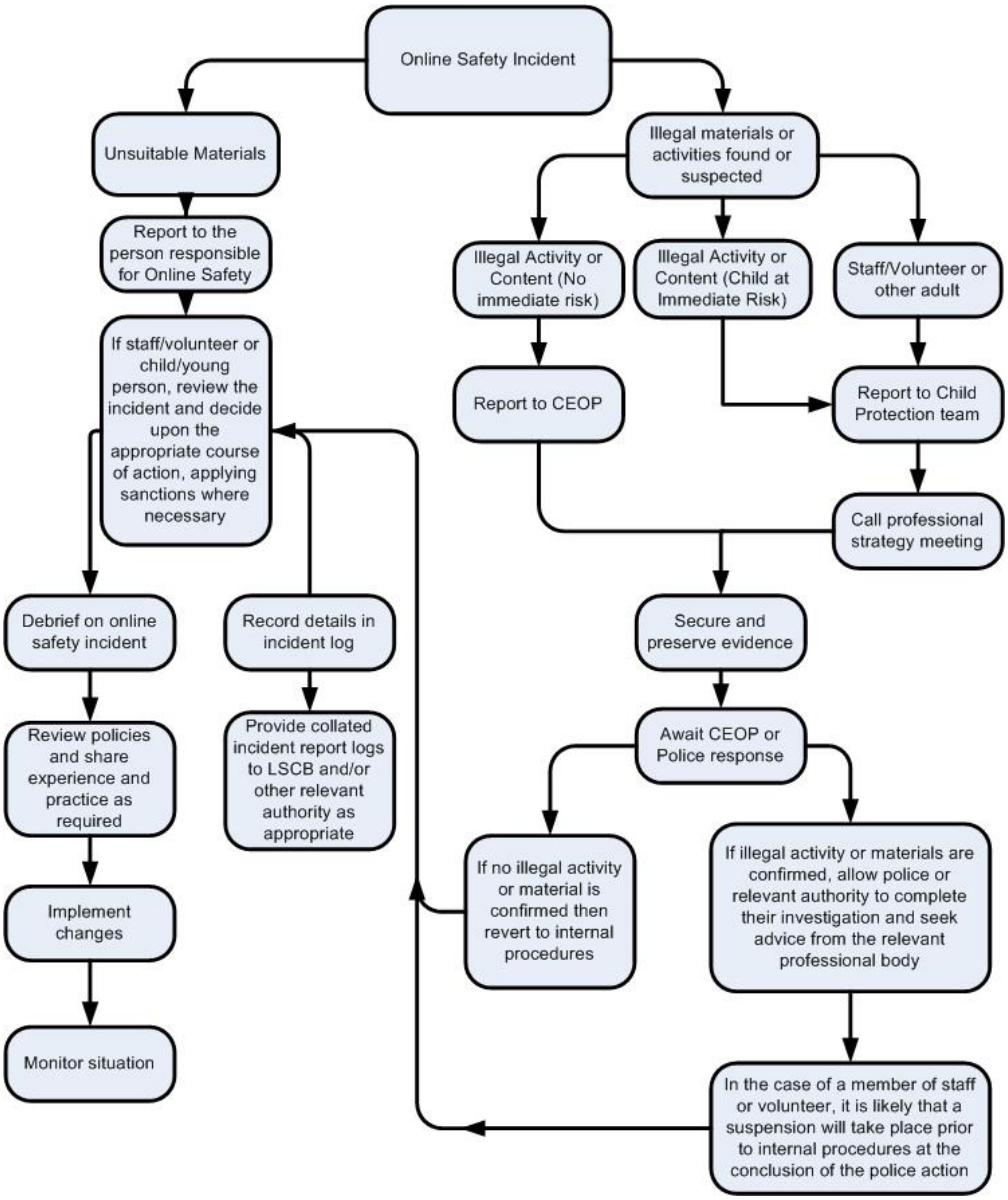
| User Actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| **Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:** | Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 | | | | | ✓ |
| | Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003. | | | | | ✓ |
| | Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008 | | | | | ✓ |
| | criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986 | | | | | ✓ |
| | pornography | | | | ✓ | |
| | promotion of any kind of discrimination | | | | ✓ | |
| | 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 | | | | ✓ | |
| Using school systems to run a private business | | | | | ✓ | |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy | | | | | ✓ | |
| Infringing copyright | | | | | ✓ | |
| 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 | | | | | ✓ | |
| Unfair usage (downloading / uploading large files that hinders others in their use of the internet) | | | | | ✓ | |
| On-line gaming (educational) | | | | | ✓ | |
| On-line gambling | | | | | ✓ | |
| On-line shopping / commerce | | | | ✓ | | |
| File sharing | | | | ✓ | | |
| Use of social media | | | | ✓ | | |
| Use of messaging apps | | | | | ✓ | |
| Use of video broadcasting eg Youtube | | | ✓ | | | |

**Responding to incidents of misuse**

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

## Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



## Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

**In the event of suspicion, all steps in this procedure should be followed:**

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation**.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

## School Actions & Sanctions

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:

# Children / Children

| Incidents: | Refer to class teacher | Refer to Head Teacher | Refer to Police | Refer to technical support staff for action re filtering / security etc | Inform parents / carers | Removal of network / internet access rights | Warning | Further sanction |
|---|---|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** | | ✓ | ✓ | | ✓ | | | |
| Unauthorised use of non-educational sites during lessons | ✓ | | | | | | ✓ | |
| Unauthorised use of mobile phone / digital camera / other mobile device | ✓ | ✓ | | | ✓ | | | |
| Unauthorised use of social media / messaging apps / personal email | | | | | ✓ | | ✓ | |
| Unauthorised downloading or uploading of files | ✓ | | | ✓ | | | | |
| Allowing others to access school network by sharing username and passwords | ✓ | | | | | | ✓ | |
| Attempting to access or accessing the school network, using another student's / pupil's account | X | | | | | | X | |
| Attempting to access or accessing the school network, using the account of a member of staff | | ✓ | | | ✓ | | | ✓ |
| Corrupting or destroying the data of other users | | ✓ | | ✓ | | | | ✓ |
| Sending an email, text or 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 breach the integrity of the ethos of the school | | ✓ | | ✓ | | | | ✓ |
| Using proxy sites or other means to subvert the school's / academy's filtering system | | ✓ | | ✓ | ✓ | | ✓ | |
| Accidentally accessing offensive or pornographic material and failing 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 Actions / Sanctions

| Incidents: | Refer to line manager | Refer to Head Teacher | Refer to Local Authority / HR | Refer to Police | Refer to Technical Support Staff for action re filtering etc | Warning | Suspension | Disciplinary action |
|---|---|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** | ✓ | ✓ | | ✓ | | | | ✓ |
| Inappropriate personal use of the internet / social media / personal email | ✓ | ✓ | | | | ✓ | | |
| Unauthorised downloading or uploading of files | ✓ | ✓ | | | ✓ | ✓ | | |
| Allowing others to access school network by sharing username and passwords or attempting to access or 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 or causing deliberate damage to hardware or software | | ✓ | | | ✓ | ✓ | | ✓ |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | | ✓ | ✓ | ✓ | | | ✓ | ✓ |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with children / children | | ✓ | ✓ | | | | | ✓ |
| 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 failing 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 | | ✓ | | | | | ✓ | ✓ |

Bussage C of E (Aided) Primary School

# Staff / Volunteer / Guest Acceptable Use Policy

**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 (eg laptops, email, website 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. ☐
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person. ☐

**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 / video 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 not use chat and social networking sites in school. ☐
- 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 on-line activity that may compromise my professional responsibilities. ☐

**The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:**

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, 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. ☐
- 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 my data is regularly backed up. ☐
- 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 disable or cause any damage to school equipment, or the equipment belonging to others. ☐
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy Where personal data is transferred outside the secure school network, it must be encrypted. ☐
- I understand that data protection policy 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. ☐

**When using the internet in my professional capacity or for school 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. ☐
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police. ☐

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.

| | |
|---|---|
| Staff / Volunteer / Guest Name | |
| Signed | |
| Date | |

Bussage C of E (Aided) Primary School

# Pupil Acceptable Use Policy: EYFS - Rainbows

**I choose to stay safe**

- I will tell an adult straight away if I see anything scary or anything that makes me feel uncomfortable online and I will not show it to other children.

**I choose to be kind and helpful**

- I will only use polite words when using the computers.

**I choose to be honest**

- I will only use the school's computers, iPads or LearnPads for things a teacher has asked me to do.

**I choose to look after property**

- I will be careful with computing equipment.
- I will tell an adult straight away if I notice computing equipment is broken or not working.

**I understand that:**

- If I do not do these things, I may not be allowed to use computers, laptops, LearnPads or other computing equipment for a period of time.

Child's Name

Signed

Date

I understand that my child has agreed to the above policy and support the school in keeping my child safe online.

Parent's Signature

Bussage C of E (Aided) Primary School

# Pupil Acceptable Use Policy: Key Stage 1

**I choose to stay safe**

- I know what my personal information is and I will not share it online. ☐
- I will tell an adult straight away if I see anything scary or anything that makes me feel uncomfortable online and I will not show it to other children. ☐
- If anyone online asks me to meet them in real life, I will tell an adult such as my teachers or parents straight away. ☐
- I will never arrange to meet anyone in person after I have met them online. ☐

**I choose to be kind and helpful** ☐

- I will only use polite language when using the computers and I will not write anything that might upset someone or give the school a bad name. ☐

**I choose to be honest**

- I will never use other people's usernames and passwords on computers left logged in by them. ☐
- I will only use the school's computer systems for things a teacher has given me permission to do. ☐
- I will not copy, remove or change any other person's files, without their knowledge and permission.

**I choose to look after property**

- I will be careful with computing equipment. ☐
- I will tell an adult straight away if I notice computing equipment is damaged. ☐

**I understand that:**

- I know that pictures on the internet can belong to the person who put them there. ☐
- I know that some things on the internet are not true. ☐
- For my own and others' safety and the safety of the school's computer systems, the school will monitor my use of the computer systems, email and other digital communications. ☐
- 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 and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information). ☐
- If I choose not to keep to this agreement I may not be allowed to use computers, laptops, LearnPads or other equipment until the school feels it is safe and right for me to do so. ☐

Child's Name

Signed

Date

I understand that my child has agreed to the above policy and support the school in keeping my child safe online.

Parent's Signature

Bussage C of E (Aided) Primary School

# Pupil Acceptable Use Policy

**I choose to stay safe**

- I will not disclose or share personal information about myself or others when online. ☐
- If I find something that I think I should not be able to see, I will turn off the screen or close the lid on a laptop or cover on a LearnPad. I will tell an adult straight away and **not show it to other children**. ☐
- I will tell an adult straight away if I see any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable online and **not show it to other children**. ☐
- I will not access or share any materials which are inappropriate or may cause harm or distress to others. If I accidentally do so, I will tell an adult straight away and **not show it to other children**. ☐
- If anyone online asks me to meet them in real life, I will tell an adult such as my teachers or parents straight away. ☐
- I will never arrange to meet anyone in person after I have met them online. ☐

**I choose to be kind and helpful** ☐

- I will only use polite language when using the computers and I will not write anything that might upset someone or give the school a bad name. ☐

**I choose to be honest**

- I will never use other people's usernames and passwords on computers left logged in by them. ☐
- I will only use the school's ICT systems for things a teacher has given me permission to do. ☐
- I will not download anything without permission. ☐
- I will not bring my own devices (mobile phones / USB devices etc) to school unless I have been given special permission by my teacher. ☐
- I will respect others' work and property and will not access, copy, remove or change any other user's files, without their knowledge and permission. ☐

**I choose to look after property**

- I will immediately report any damage or faults involving equipment or software, however this may have happened. ☐
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes. ☐
- I will not install or attempt to install programmes, or store programmes on a school computer, nor will I try to alter computer settings. ☐
- I will not attempt to use the school's ICT systems for file-sharing. ☐

**I understand that:**

- I will acknowledge sources of information and images copied from the internet using a reference. ☐
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may be incorrect and may even be a deliberate attempt to mislead me. ☐
- For my own and others' safety and the safety of the school's ICT systems, the school will monitor my use of the ICT systems, email and other digital communications. ☐
- 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 and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information). ☐
- If I choose not to keep to this agreement I may not be allowed to use computers, laptops or other equipment until the school feels it is safe and right for me to do so. ☐

Child's Name

Signed

Date

I understand that my child has agreed to the above policy and support the school in keeping my child safe online.

Parent's Signature