Online Safety Policy

Our Vision

Bells Farm Primary School embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, Bells Farm Primary School aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

Development / Review of this Policy

This online safety policy has been developed by the Digital Council made up of:

- SLT
- Online Safety Coordinator
- Staff – including Teachers, Support Staff, Technical staff
- Governors
- Parents and Carers
- Community users

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Scope

This policy applies to all members of the school community (including staff, students, 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 Headteachers to such extent as is reasonable, to regulate the behaviour of students 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 outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Publicising Online Safety

Effective communication across the school community is key to achieving the school vision for safe and responsible citizens. To achieve this we will:

- Make this policy, and related documents, available on the school website at: http://www.bellsfrm.bham.sch.uk and http://www.bellsfarm.org
- Introduce this policy, and related documents, to all stakeholders at appropriate times. This will be at least once a year or whenever it is updated
- Post relevant Online Safety information in all areas where computers are used
- Provide Online Safety information at parents evenings and through the school newsletter

Roles and Responsibilities

The following section outlines the Online Safety roles and responsibilities of individuals and groups within the *school.*

Governors

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

- regular meetings with the Online Safety Co-ordinator
- regular monitoring of Online Safety incident logs from CPOMS
- regular monitoring of filtering / change control logs

• reporting to relevant Governors meeting

Headteacher and Senior Leaders

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the *Online Safety Co-ordinator.*

- The Headteacher and (at least) another member of the Senior Leadership Team 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.
- The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.

Online Safety Co-ordinator (Mr Baddhan)

- leads the Online Safety committee (Digital Council)
- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments
- meets regularly with Online 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

ICT Operations Manager (Mr Baddhan)

- The ICT Operations Manager 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 Online Safety technical requirements and any Local Authority / other relevant body Online 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
- that they keep up to date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader; Online Safety Coordinator
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

- they have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher / Senior Leader ; Online Safety Co-ordinator for investigation / action / sanction
- all digital communications with students / parents / carers should be on a professional level and only carried out using official school systems
- Online Safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the Online Safety and acceptable use policies
- students 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 students 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 Officer

should be trained in Online 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

Digital Council

The Digital Council (Online Safety Group) provides a consultative group that has wide representation from the *school* community, with responsibility for issues regarding Online Safety and the monitoring the Online Safety policy including the impact of initiatives. Depending on the size or structure of the *school* this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the *Governing Body*.

Members of the *Digital Council* will assist the *Online Safety Co-ordinator* with:

- the production / review / monitoring of the school Online Safety policy / documents.
- mapping and reviewing the Online Safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students about the Online Safety provision
- monitoring improvement actions identified through use of the 360 degree safe self review tool
- A Digital Council Terms of Reference is agreed by all members of the group and is also available in the Media Centre.

Students

- are responsible for using the *school* digital technology systems in accordance with the Student 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 Online Safety practice when using digital technologies out of school and realise that the *school's* Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

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

- digital and video images taken at school events
- access to parents' sections of the website and on-line student / pupil records
- their children's personal devices in the school (where allowed)

Community Users

Community Users who access school systems 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 – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. At Bells Farm, the education of students 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.

Bells Farm commits to Online Safety in all areas of the curriculum and staff reinforce Online Safety messages across the curriculum. The Online Safety curriculum is broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned Online Safety curriculum is provided as part of Computing / PHSE / other lessons and will be regularly revisited
- Key Online Safety messages are be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students are 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.
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

• Students will be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
• Staff will act as good role models in their use of digital technologies the internet and mobile devices

• in lessons where internet use is pre-planned, it is best practice that students 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 students are allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites the young people visit.
• It is accepted that from time to time, for good educational reasons, students may need to research topics (eg 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 Online 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.

Bells Farm will therefore seek to provide information and awareness to parents and carers through:
• Curriculum activities
• Letters, newsletters, website, class blogs
• Parents evenings / sessions
• High profile events / campaigns eg Safer Internet Day

Education – The Wider Community
The school will provide opportunities for local community groups / members of the community to gain from the school's Online Safety knowledge and experience. This may be offered through the following:
• Providing family learning courses in use of new digital technologies, digital literacy and Online Safety
• Online Safety messages targeted towards grandparents and other relatives as well as parents.
• The school website will provide Online Safety information for the wider community

• Supporting community groups eg Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online Safety provision

Education & Training – Staff / Volunteers
It is essential that all Bells Farm staff receive Online Safety training and understand their responsibilities, as outlined in this policy.

Training will be offered as follows:
• A planned programme of formal Online Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the Online Safety training needs of all staff will be carried out regularly.
• All new staff will receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Agreements.
• The Online Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events (eg from LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
• This Online Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
• The Online Safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors
Bells Farm Governors will also take part in Online Safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in technology / Online 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 or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring
Bells Farm internet connection is managed through the local authority's recommended internet provider. The local authority ensures and carries out all the Online Safety measures as suggested below.

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 Online Safety responsibilities:

• School technical systems will be managed in ways that ensure that the school meets recommended technical requirements (these may be outlined in Local Authority / other relevant body policy and guidance)
• There will be regular reviews and audits of the safety and security of school technical systems
• Servers, wireless systems and cabling must be securely located and physical access restricted
• All users will have clearly defined access rights to school technical systems and devices.
• All users (at KS2 and above) will be provided with a username and secure password by Mr Baddhan who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every 6 months. KS1 use shared passwords until they reach KS2 where they will receive their own unique password.
• The “master / administrator” passwords for the school ICT system, used by the ICT Operations Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)
• Mr Baddhan 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 (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
• Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the local authority by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
• The school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / students etc)
• School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
• An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
• Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, 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” (eg trainee teachers, supply teachers, visitors) onto the school systems.
• An Acceptable Use Policy is in place that forbids staff from downloading executable files and installing programmes on school devices.
• An Acceptable Use Policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices (see below). Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Removable Media (eg memory sticks / CDs / DVDs)

- The use of removable media is not prohibited within Bells Farm; it is infact an essential part of everyday work.
- The use of removable media to transport non-sensitive data can be done on standard devices (see above for details).
- Regularly updated Antivirus software will be present on all machines from which the data is taken from and machines on which the data is to be loaded.
- When removable media is used to transport sensitive data, the data on the device must be encrypted to a recommended encryption standard (AES-256).
- Mobile devices and/or removable storage containing sensitive or highly sensitive data will not be sent off site without prior agreement.
- If highly sensitive data is required to be transported via removable media please seek advice from Mr Baddhan or Mrs Butterworth.
- Any sensitive or highly sensitive data transferred to a removable media device must remain encrypted and must not be transferred to any external system in an unencrypted form.
- The user must note and accept that should their encryption password be forgotten, the removable device allows for a new password to
- be created, but this will involve a reformatting of the device and thus a total loss of the data. The removable device must therefore not be used to keep data that is not backed-up security in a central location.
- Removable media should be physically protected against loss, damage, abuse or misuse when in use, storage and transit.
- Mobile devices and/or removable media that have become damaged should be handed back to Mr Baddhan to ensure it is disposed of securely to avoid data leakage.
- If a member of staff who uses a school removable disk, they should return the device to the school for secure destruction and/or redistribution.

Bring Your Own Device (BYOD)
The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability.

Bells Farm allows the use of BYOD however, please refer to the BYOD policy for further details.

Use of digital and video images
The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students 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.

Our 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 will inform and educate students 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 eg 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 students 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 students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
• Students must not take, use, share, publish or distribute images of others without their permission
• Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
• Students' 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 students are published on the school website
• Student's work can only be published with the permission of the student / pupil and parents or carers.

Prevent Duty
Since 1st July 2015, all schools are subject to a duty under section 26 of the Counter—Terrorism and Security Act 2015 to have due regard to prevent people from being drawn into terrorism. This duty is known as the Prevent duty. Bells Farm ensure staff are trained to be able to identify children who may be vulnerable to radicalisation, and what to do when they are identified. As a school we ensure children are safe from terrorist and extremist material when accessing the internet in school by filtering and monitoring software. At Bells Farm we equip our children to stay safe online both in school and outside. Internet safety is integral to the school's Online Safety curriculum and is also embedded with the PSHE subject to explore controversial issues, and equipping them with the knowledge and skills to understand and manage difficult situations. Schools are already expected to promote the spiritual, moral, social and cultural developments and, with this, fundamental British values.

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.

Following a number of “high profile” losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data.

Bells Farm 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”. (see Privacy Notice section in the appendix)
- 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)
- Risk assessments are carried out
- 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 – see the Cloud Storage policy for more.

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.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

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				Students			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission and supervision	Not allowed
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	✓						✓	

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 will be aware that email communications are monitored. Staff and students will therefore use only the school email service to communicate with others when in school, or on school systems.

• Users must immediately report, to Mrs Butterworth or Mr Baddhan – 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 students or parents / carers (email, chat 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 social media must not be used for these communications.

• Whole class / group email addresses may be used at KS1, while students at KS2 and above will be provided with individual school email addresses for educational use.

• Students will be taught about Online Safety issues, such as the risks attached to the sharing of personal details. They will 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 students 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.

Bells Farm provide the following measures to ensure reasonable steps are in place to minimise risk of harm to students, 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 will ensure that:

- No reference will be made in social media to students, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions will 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 safeguarding officer and Online Safety committee.

Staff are trusted to use digital technologies and social networking sites through regular training and advice.

Unsuitable / inappropriate activities

Bells Farm believe 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:

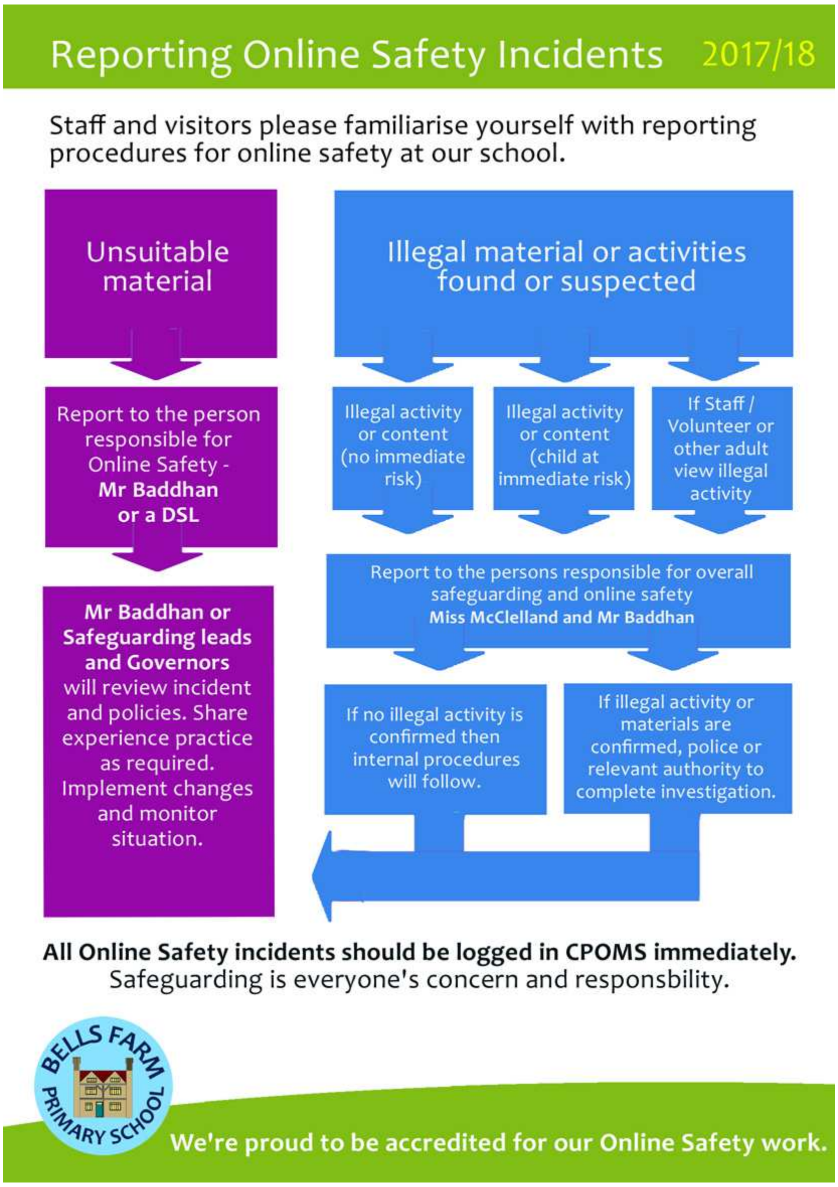
User Actions

		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,	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	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					X

remarks, proposals or comments that contain or relate to:	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	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				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non educational)				X		
On-line gambling						X
On-line shopping / commerce					X	
File sharing					X	
Use of social media (Twitter, YouTube, Google+)			X			
Use of messaging apps					X	
Use of video broadcasting eg Youtube			X			

Responding to incidents of misuse
This guidance is intended for use when staff or visitors 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.

Illegal and Unsuitable 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) for responding to online safety incidents and report immediately to the police.



Reporting Online Safety Incidents 2017/18

Staff and visitors please familiarise yourself with reporting procedures for online safety at our school.

Unsuitable material

Report to the person responsible for Online Safety - **Mr Baddhan or a DSL**

Mr Baddhan or Safeguarding leads and Governors will review incident and policies. Share experience practice as required. Implement changes and monitor situation.

Illegal material or activities found or suspected

Illegal activity or content (no immediate risk)

Illegal activity or content (child at immediate risk)

If Staff / Volunteer or other adult view illegal activity

Report to the persons responsible for overall safeguarding and online safety **Miss McClelland and Mr Baddhan**

If no illegal activity is confirmed then internal procedures will follow.

If illegal activity or materials are confirmed, police or relevant authority to complete investigation.

All Online Safety incidents should be logged in CPOMS immediately.
Safeguarding is everyone's concern and responsbility.

We're proud to be accredited for our Online Safety work.

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 will 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 will be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behavior
- 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 will 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:

Students Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Online Safety Coordinator	Refer to Headteacher	Refer to Police	Refer to Mr Baddhan for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					X
Unauthorised use of non-educational sites during lessons	X				X	X		X	
Unauthorised use of mobile phone / digital camera / other mobile device	X		X			X		X	
Unauthorised use of social media / messaging apps / personal email	X	X			X	X			
Unauthorised downloading or uploading of files	X				X	X			
Allowing others to access school network by sharing username and passwords	X						X	X	
Attempting to access or accessing the school network, using another student's / pupil's account	X						X	X	
Attempting to access or accessing the school network, using the account of a member of staff	X					X	X	X	
Corrupting or destroying the data of other users			X				X	X	

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X	X		X		X	X
Continued infringements of the above, following previous warnings or sanctions			X	X		X			X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X		X					X
Using proxy sites or other means to subvert the school's filtering system	X	X		X					X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X							
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X					X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X					X	

Staff Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Mr Baddhan 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).	X	X	X	X		X	X	X
Inappropriate personal use of the internet / social media / personal email		X				X		
Unauthorised downloading or uploading of files	X	X			X	X		
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	X	X			X	X		
Careless use of personal data eg holding or transferring data in an insecure manner	X	X			X	X		X

Deliberate actions to breach data protection or network security rules	X	X			X		X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X			X		X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X		X				X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students		X		X		X		X
Actions which could compromise the staff member's professional standing		X		X		X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X				X		X
Using proxy sites or other means to subvert the school's filtering system	X	X			X		X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X		X
Deliberately accessing or trying to access offensive or pornographic material	X	X			X		X	
Breaching copyright or licensing regulations	X	X	X		X	X	X	
Continued infringements of the above, following previous warnings or sanctions	X	X	X				X	

Date of review June 2017

Next review July 2018