**Bawtry Mayflower Primary School**

# Online Safety Policy

Review date: Summer 2020

This policy applies to all members of the school (including staff, students / pupils, 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. 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.

## Policy Statement

For clarity, the online safety policy uses the following terms unless otherwise stated:

Users – refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents and Carers - any adult with a legal responsibility for the child/ young person outside the school. E.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences school trips etc.

Wider school community – students, all staff, governing body, parents, clubs.

Safeguarding is a serious matter. At Bawtry Mayflower Primary School, we use technology and the internet extensively across all areas of the curriculum. Online safeguarding is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an online safety incident.

The primary purpose of this policy is twofold:

1. To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.

2. To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the school's website; upon review all members of staff will sign as read and understand, and agree to follow both the online safety policy and the Staff Acceptable Use policy.

At the beginning of each school year, the children will receive a letter with a permission slip that must be signed; this says that the children and parents/carers will adhere to the acceptable use policy. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the internet.

# Roles and Responsibilities

### Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place, as such they will:

Review this policy annually and in response to any online safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing these incidents.

Our governors will:

- Keep up to date with the emerging risks and threats through technology use
- Receive updates as appropriate from the head teacher in regards to training, identified risks and any incidents.
- Receive updates from the Online Safety Lead

### Head teacher and Senior Leaders

Reporting to the governing body, the head teacher has overall responsibility for online safety within our school. The day to day management of this will be delegated to a member of staff, the online safety lead, as indicated below.

The Head teacher will ensure that:

Online safety training throughout the school is planned and up to date and appropriate to the recipient, e.g. students, all staff, SLT and governing body, parents.

The designated online safety lead has had appropriate CPD in order to undertake the day to day duties. The Headteacher and 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.

All online safety incidents are dealt with promptly and appropriately. The Headteacher and another member of the Senior Leadership Team (**Rebecca Parkes)** should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents later in this policy)

### Online Safety Lead

The day to day duty of online safety officer is devolved to: **Rebecca Parkes**

The online safety officer will:

Keep up to date with the latest risks to children whilst using technology; familiarise him/ herself with the latest research and available resources for school and home use.

Take day to day responsibility for online safety issues and has a leading role in establishing and reviewing this policy regularly along with other related document and bring any matters to the attention of the Head teacher. Advise the Head teacher and governing body on all online safety matters.

Provides training and advice for staff and ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place

Retain responsibility for ensuring that all online safety incidents are logged appropriately on CPOMS and these are dealt with appropriately to inform future online safety developments.

Engage with parents and the school community on online safety matters at school and/or home.
Liaise with the local authority, IT technical support and other agencies as required.

Ensure any technical online safety measures in school (e.g. internet filtering software, behaviour management software) are fit for purpose through liaison with the LA and ICT technical support.

Reports regularly to the Senior Leadership Team and in partnership with them decides on the investigation/ action and sanctions process for any online safety incidents.

**ICT Technical Support Staff**

Technical support staff (Impelling Solutions) are responsible for ensuring that the IT technical infrastructure is secure.

**All Staff**

Staff are to ensure that:

All details within this policy are understood. If anything is not understood it should be brought to the attention of the head teacher or online safety officer.

They have an up to date awareness of online safety matters and the current school policy and practices.
They have read, understood, signed and abide by the acceptable use policy.

All digital communication with pupils and parents/ carers should be on a professional level and only carried out using official school systems.

Online safety issues are embedded in all aspects of the curriculum and other activities and implement current policies with regard to the use of digital technologies, mobile devices, cameras etc in lessons.

Pupils understand and follow the online safety and acceptable use policies and have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

In lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Any online safety incident is to be reported to the online safety lead, and/ or the head teacher and recorded as an online safety incident on CPOMS.

The reporting flowcharts contained within this online safety policy are to be understood.

**EYFS**

All staff are aware of the UKCIS framework (Education for a Connected World) which provides information about the skills and competences that children and young people need to have with regards to online safety from the age of 4 upwards.

The children receive age appropriate, progressive and embedded online safety education throughout the curriculum.

## **Parents and Carers**

The school will offer parents the skills and knowledge they need to promote online safety of children outside the school environment. Through parent’s evenings, school newsletters, regular promotion and links on our website, the school will keep parents up-to-date with new and emerging online safety risks and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student acceptable use policy to show support of the policies and procedures before any access can be granted to school ICT equipment or services. They will also sign a parent's AUP policy at the start of each school year.

## Education - All Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety 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.

The boundaries of use of the ICT equipment and services in this school are given in the student acceptable use policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance to the behaviour policy.

## Technology

Bawtry Mayflower Primary School uses a range of devices including but not limited to: Ipads, Cameras, PCs and Laptops. The school will be responsible for ensuring that the school network is as safe and secure as 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.

There will be regular reviews and audits of the safety and security of school technical systems. All users will have clearly defined access rights to school technical systems and devices.

Students, visitors and guests will be provided with information on a guest log in and guest wifi access as appropriate.

The school Business Manager and IT technical support are 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.** We use an educational filtered system that prevents unauthorized access to illegal websites. Illegal content (including child sexual abuse images) is filtered by the broadband or filtering provider. Content lists are regularly updated and internet use is logged and regularly monitored. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident; whichever is sooner. The ICT co-ordinator, online safety officer and IT support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the head teacher.

**Passwords:** All staff will be unable to access a device that can access personal or confidential data without a unique username and password. The ICT co-ordinator and IT support are responsible for ensuring that these are kept secure.

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.

## Safe Use

**Internet:** Use of the internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this online safety and the staff acceptable use policy; pupils (or their parents) upon signing and returning their acceptance of the acceptable use policy.

**Email:** All staff are reminded that their emails are subject to Freedom of Information Requests, and as such the email service is to be used for professional work based emails only. Emails of a personal nature are not permitted. Similarly use of personal emails for work purposes are not permitted.

**Incidents:** Any online safety incident is to be brought to the immediate attention of the head teacher and online safety officer.

**Use of digital and video images**

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 students / pupils 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 / pupils* 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.

Pupils must not take, use, share, publish or distribute images of others without their permission

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' 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 pupils are published on the school website (covered as part of the AUP signed by parents or carers at the start of the year.

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
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

**Communications**

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.
- 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 students / pupils or parents / carers 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.
- Pupils should be taught about online 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**

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, 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 is in place.

School staff should ensure that:

- No reference should be made in social media to students / pupils, 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.

**Unsuitable / inappropriate activities**

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities eg cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

We encourage the children to use social media appropriately and in accordance with this policy. All children should abide by the age restrictions on different social media sites/games in order to safeguard them.

**PREVENT**

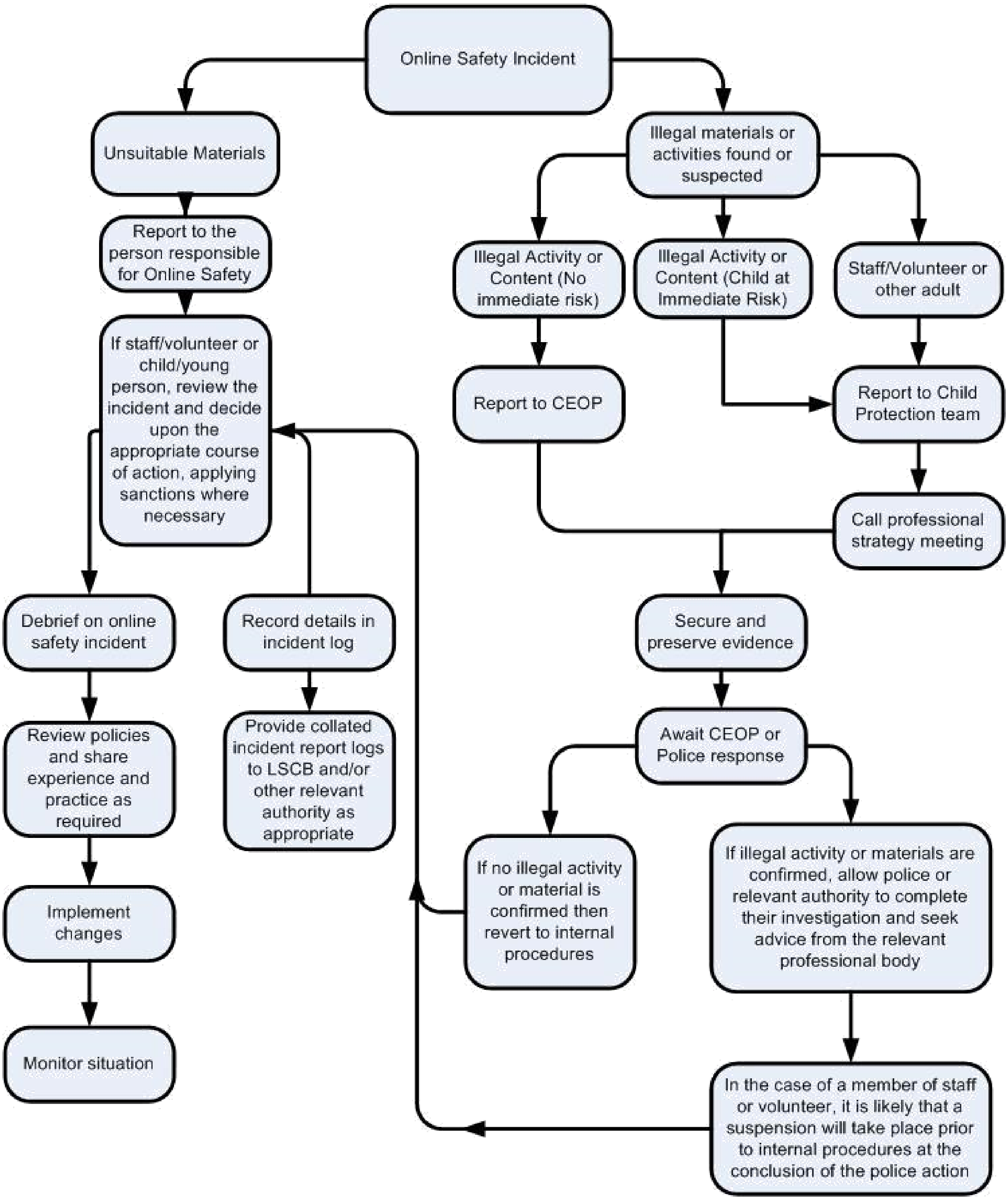
In accordance with the Prevent Strategy, which aims to prevent children and young people being exposed to extremist views and at risk of radicalisation, staff are all trained on the channel programme http://course.ncalt.com/Channel_General_Awareness/01/index.html

This responsibility extends to online safety and protecting children from extremist material online. Through this training, staff are aware of how the internet is used to radicalise people. Filtering should prevent access to such extremist sites but any material accessed at school should be treated as an online safety incident and dealt with accordingly. Disclosures or concerns regarding exposure outside of school should be treated as a safeguarding incident and dealt with in accordance with the Safeguarding policy and procedures (cf. Safeguarding policy).

Parents and carers are informed about the risks of radicalisation and extremism via online safety newsletters and The Prevent Action Plan which is available the school website.

**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 for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

## 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.

## 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 in conjunction with the school’s behaviour policy.