

Inspiring and flourishing together

Lightcliffe C of E Primary School

# **POLICIES & PROCEDURES**

## **Online Safety Policy**

Date Policy Approved: 24<sup>th</sup> November 2022

Approving Body: MAT Board

Next Review Date: 23<sup>rd</sup> November 2024

Previous Review Date: Spring 2020



## Contents

1. Introduction and Aims.....	3
2. Legislation and guidance.....	4
3. Roles and responsibilities .....	4
4. Educating pupils about online safety .....	9
5. Educating parents about online safety .....	9
6. Cyber-bullying.....	10
7. Acceptable use of the internet in school .....	12
8. Pupils using mobile devices in school .....	12
9. Staff using work devices outside school.....	12
10. How the school will respond to issues of misuse .....	13
11. IT Systems .....	13
12. Using the Internet and Email .....	14
13. Publishing content online .....	15
14. Training .....	16
15. Monitoring arrangements .....	17
16. Links with other policies .....	17
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers) .....	198
Appendix 2: KS2 acceptable use agreement (pupils and parents/carers).....	19
Appendix 3: Acceptable use agreement (staff, governors, volunteers and visitors).....	20
Appendix 4: online safety training needs – self audit for staff.....	21
Appendix 5: online safety incident report log.....	22
Appendix 6: Web filtering and e-safety.....	23

---

# 1. Introduction and Aims

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies staff, children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Making /receiving phone calls via their mobile phones
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

This online safety policy recognises the commitment of our school to online safety and acknowledges its part in the school's overall Safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep pupils safe when using technology. We believe the whole school community can benefit from the opportunities provided by the Internet and other technologies used in everyday life. The online safety policy supports this by identifying the risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities.

Abbey Multi Academy Trust aims to ensure its academies:

Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors

Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')

Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

## The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

**Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism

**Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

**Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

**Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

## 2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study and complies with our funding agreement and articles of association.

## 3. Roles and responsibilities

### 3.1 The governing body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Richard Monro.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures

- Read, understand, contribute to and help promote the school's online safety policies and guidance as part of the school's overarching Safeguarding procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in online safety awareness
- To have an overview of how the school IT infrastructure provides safe access to the internet and the steps the school takes to protect personal and sensitive data
- Ensure appropriate funding and resources are available for the school to implement their online safety strategy

### **3.2 The Headteacher**

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. The headteacher will:

- Ensure liaison with the Governors
- Develop and promote an online safety culture within the school community
- Ensure that all staff, pupils and other users agree to the Acceptable Use Policy and that new staff have online safety included as part of their induction procedures
- Receive and regularly review online safety incident logs; ensure that the correct procedures are followed should an online safety incident occur in school and review incidents to see if further action is required

### **3.3 The designated safeguarding lead**

Details of the school's DSL and deputies are set out in our Child Protection and Safeguarding Policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school anti-bullying policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

### **3.4 The ICT manager / IT Technical Staff**

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on an ongoing basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Support the school in providing a safe technical infrastructure to support learning and teaching
- Ensure appropriate technical steps are in place to safeguard the security of the school ICT system, sensitive data and information. Review these regularly to ensure they are up to date
- Ensure that provision exists for misuse detection and malicious attack
- Report any online safety related issues that come to their attention
- Ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems, including password management
- Ensure that suitable access arrangements are in place for any external users of the school's ICT equipment.
- Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

This list is not intended to be exhaustive.

### 3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy Read, understand and help promote the school's eSafety policies and guidance
- Taking responsibility for ensuring the safety of sensitive school data and information
- Developing and maintaining an awareness of current online safety issues, legislation and guidance relevant to their work
- Maintaining a professional level of conduct in their personal use of technology at all times
- Ensuring that all digital communication with pupils is on a professional level and only through school based systems, NEVER through personal email, text, mobile phone social network or other online medium.
- Embedding online safety messages in learning activities where appropriate
- Supervising pupils carefully when engaged in learning activities involving technology
- Ensuring that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Reporting all online safety incidents which occur in the appropriate log and/or to their line manager
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

### 3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)
- Help and support the school in promoting online safety

- Discuss online safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Consult with the school if they have any concerns about their child's use of technology
- Support the school approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - [UK Safer Internet Centre](#)
- Hot topics - [Childnet International](#)
- Parent factsheet - [Childnet International](#)
- [Healthy relationships – Disrespect Nobody](#)

### 3.7 Pupils

We expect pupils to:

- Take responsibility for their own and each other's' safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
- Ensure they respect the feelings of other pupils
- Ensure they respect the rights of other pupils
- Ensure they respect the values of others in their use of technology in school and at home
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all online safety incidents to appropriate members of staff
- Discuss online safety issues with family and friends in an open and honest way
- To know, understand and follow school policies on the use of mobile phones, digital cameras and handheld devices
- To know, understand and follow school policies regarding bullying
- Pupils will support the school approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute.

### 3.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).



## 4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

**Primary schools:**

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The safe use of social media and the internet will also be covered in other subjects where relevant.
- Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

## 5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website and Class Dojo. This policy will also be shared with parents.

The school will let parents know:

- What systems the school uses to filter and monitor online use

- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

## **6. Cyber-bullying**

### **6.1 Definition**

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school positive behaviour policy.)

### **6.2 Preventing and addressing cyber-bullying**

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school positive behaviour / anti-bullying policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

### **6.3 Examining electronic devices**

The headteacher, and any member of the senior leadership team authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or

- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher and /or DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

## **7. Acceptable use of the internet in school**

All pupils, parents, staff, volunteers, trustees and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, trustees, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

## **8. Pupils using mobile devices in school**

Year 6 pupils are permitted to bring mobile phones into school once a parent has completed an online consent and agreement form. Phones are collected as the pupils arrive in school, then kept in the school office and handed back as the pupils leave at the end of the day.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

## **9. Staff using work devices outside school**

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

The Trust ensures that all laptops provided for use inside and outside school have:

- Anti-virus and anti-spyware software installed
- Up-to-date operating systems with the latest updates installed

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from a member of IT support.

If you are provided an iPad the Trust, you will be required to read and sign a Digital Device Policy which contains further details specific to that device.

## **10. How the school will respond to issues of misuse**

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

## **11. IT Systems**

The school decides which users should and should not have Internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary log in.

All users are provided with a log in appropriate to their key stage or role in school. Pupils are taught about safe practice in the use of their log in and passwords.

Staff are given appropriate guidance on managing access to laptops which are used both at home and school and in creating secure passwords.

Access to personal, private or sensitive information and data is restricted to authorized users only, with proper procedures being followed for authorizing and protecting login and password information.

### **11.1 Passwords**

- We ensure that a secure and robust username and password convention exists for all system access (email, network access, school management information system).
- We provide all staff with a unique, individually-named user account and password for access to IT equipment, email and information systems available within school.
- All pupils have a unique, individually-named user account and password for access to IT equipment and information systems available within school.

- All staff and pupils have responsibility for the security of their usernames and passwords and are informed that they must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains a log of all accesses by users and of their activities while using the system in order to track any eSafety incidents.
- Password must be difficult to guess and should be a mixture of upper case and lowercase, numbers and symbols. strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Pupils will have to reset their passwords at given intervals.

## **12 Using the Internet and Email**

### **12.1 Internet**

We provide the internet to:

- Support curriculum development in all subjects
- Support the professional work of staff as an essential professional tool
- Enhance the school's management information and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with the examination boards and others

Users are made aware that they must take responsibility for their use of, and their behaviour whilst using the school IT systems or a school provided laptop or device and that such activity can be monitored and checked.

### **12.2 Using Email**

Email is regarded as an essential means of communication and the school provides all members of the school community with an e-mail account for school based communication. Communication by email between staff, pupils and parents will only be made using the school email account and should be professional and related to school matters only. E-mail messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained.

All email activity is recorded in line with data protection laws. The school is able to view these records in situations where this is called upon.

It is the personal responsibility of the email account holder to keep their password secure.

As part of the curriculum pupils are taught about safe and appropriate use of email. Pupils are informed that misuse of email will result in a loss of privileges.

School will set clear guidelines about when pupil-staff communication via email is acceptable and staff will set clear boundaries for pupils.

Under no circumstances will staff contact pupils, parents or conduct any school business using a personal email addresses.

Responsible use of personal web mail accounts on school systems is permitted for staff only outside teaching hours.

## **12.3 Receiving Emails**

- Check your e-mail regularly
- Activate your 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source

## **13 Publishing content online**

### **13.1 School Website:**

The school maintains editorial responsibility for any school initiated web site or publishing online to ensure that the content is accurate and the quality of presentation is maintained. The school maintains the integrity of the school website by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the web site is the school address, e-mail and telephone number.

Identities of pupils are protected at all times. Parents have the option to opt out so that photographs of individual pupils are not published on the website. Group photographs do not have a name list attached.

### **13.2 Online Material Published Outside the School:**

Staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school as they are in school.

Material published by pupils, governors and staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of another pupil or member of the school community will be considered a breach of school discipline and treated accordingly.

Further information can be found in the Safe Working Practice Guidance.

### **13.3 Using Images, Video and Sound**

We recognize that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants and their parents; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress.

In line with GDPR regulations, we will ask all parents/carers to give permission for their child to be photographed or videoed (in publications and on websites) when they start at the academy and at periodic intervals. Parents / carers will be able to opt-out at any time should they wish to do so.

For their own protection staff or other visitors to school never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils.

We are happy for parents to take photographs at school events, except in specific circumstances where rights holders refuse permission, but will always make them aware that they are for personal use only and if they have taken photographs of children other than their own they should not be uploaded to social media sites and can be only used for their personal use.

## 14. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, harassing, and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.



## **15. Monitoring arrangements**

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Co-CEO (operations). At every review, the policy will be shared with the trust board and governing body. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

## **16. Links with other policies**

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Positive Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Digital Device Policy

## ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
  - I click on a website by mistake
  - I receive messages from people I don't know
  - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

**Parent/carer agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

## Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

### ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

**I will read and follow the rules in the acceptable use agreement policy**

**When I use the school's ICT systems (like computers) and get onto the internet in school I will:**

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

**I will not:**

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

**If I bring a personal mobile phone or other personal electronic device into school:**

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**

Signed (pupil):

Date:

**Parent/carer's agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

### Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

#### ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date:

#### Appendix 4: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the way pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

Designed especially for schools

Web Filtering & eSafety

## The most advanced web filters available

**Our hosted web filtering solution from Netsweeper, provides the world's most accurate and comprehensive filtering classification system, for protecting students and staff from unacceptable online content.**

### Supports DfE compliance

Developed specifically for education, we filter billions of categorised URLs, including the Internet Watch Foundation lists and the Home Office Terrorism block list. As such, our filters fully meet school Prevent Duty and DfE regulatory requirements.

Automated real-time filtering updates, protect students from harmful content almost as quickly as it is created.

### Fully customisable control

Providing central filtering control for multi-site schools, control in the classroom, or mobile device management, we provide the flexibility to manage granular filtering policies by user, group, time and day, on and off site.

### Reporting

We allow you to view up to 6 months' worth of historical internet usage and our own back-up system will extend this to 3 years. This information can then be presented to the authorities or the police if required.



**Find out more. Call or email:**  
**01133 222 333 | [info@schoolsbbroadband.co.uk](mailto:info@schoolsbbroadband.co.uk)**



## The Benefits

**Our unique hosted platform offers scalability for growth, with zero additional hardware costs.**

Safe search across all popular web search engines including Google, Bing and YouTube

Add your own URLs, keywords, file extensions and URL rewrites

Easy to use real-time and predefined reporting

Powerful custom reports and alerts

Filter activity on hundreds of social media platforms

Tailor internet access by user, IP address, group or domain

Block or allow websites for set periods of time

View historic internet use

Meets Prevent Duty requirements

Integrates with Windows Active Directory, Mac Open Directory, Azure, Google and GSuite

Protecting both students and staff from inappropriate online content, the service supports schools' Prevent Duty compliance and KCSIE duties through its easy to use, built-in monitoring, reporting and alert functions.

We also offer a full 4G Filtered service with preconfigured routers/dongles for a "ready to go" experience.

Service delivered via either: SIM Card | Dongle | MiFi Capable Router

Available in monthly data plan increments from 1Gbps to 10Gbps

Rapid provisioning

Short & longer term flexible contracts

**Find out more. Call or email:**

**01133 222 333 | [info@schoolsbbroadband.c](mailto:info@schoolsbbroadband.c)**

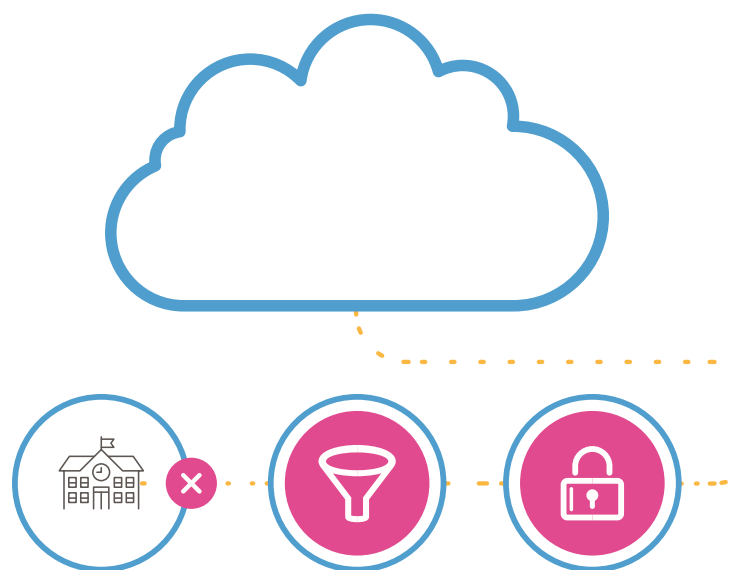
## Effective BYOD Filtering

**Web filtering for mobile devices on or off school sites.**

Schools Broadband mobile filtering allows you to extend your existing filtering policies to your off-network devices. This includes Apple devices, Chromebooks, Netbooks, laptops, Windows tablets, android devices and mobile phones.

The Mobile filter offers exactly the same level of protection and reporting as on-site devices, transparently communicating Internet browser requests from a mobile device to our cloud-based filtering system.

This system references the URL requests with its content data-base and policy settings and either allows or blocks the request.



## 4G Filtered Broadband For Safe

### Internet Access At Home

**Now that the DfE SIM plans for mobile filtered data have ended, you can still use your existing DfE supplied MiFi routers/dongles with our SIM only solution.**

Our mobile filtering and SIM-only service is designed exclusively for education, providing a safe and filtered learning environment for student home-learning.

