Abbotswood Junior School

Online safety policy

Approved by:	**Headteacher**	**Date: Autumn 2025**
Last reviewed on:	**Autumn Term 2025**	
Next review due by:	**Autumn Term 2026**	

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- 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, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **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 scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) 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
- Relationships and sex education
- 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.

3. Roles and responsibilities

3.1 The governing board

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

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will coordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL) and deputy designated safeguarding leads (DDSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Matt Stevens.

All governors will:

- Ensure 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

- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is 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

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.

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL/ DDSLs 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 and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- 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's child protection policy
- Ensuring that any online safety incidents are logged on CPOMS 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 behaviour policy
- Updating and delivering staff training on online safety
- 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
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually 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 any Senso alerts are shared with the DSL/ DDSL so that these can be addressed
- Meeting with the DSL/ DDSLs regularly to review the filtering and monitoring systems on school devices
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

- Conducting regular security checks and continuously monitoring the school's ICT systems to keep them secure.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on CPOMS 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

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)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting this to a member or to the school's IT manager.
- Following the correct procedures by asking the IT manager to alter a filter if they need to bypass the filtering and monitoring systems for educational purposes; for example, adapting a filter so that a term is not 'flagged' only for the duration of that topic.
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS 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
- 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/carers

Parents/carers are expected to:

- Notify a member of staff, DSL/ DDSL or the headteacher of any concerns or queries regarding this policy
- Understand that their child will read, have understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1 and 2) when children sign the Abbotswood Technology Charter.

Parents/carers 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
- Parent/ carer resource sheet – Childnet
- Parents/ carers can also look on the Online Safety section of the school website.

3.7 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 and the National Curriculum computing programmes of study. Pupils are also taught about online safety within teaching about relationships education, relationships and sex education (RSE) and health education.

In **Key Stage (KS) 1**, before joining Abbotswood, pupils will be taught to:

- Use technology safely and respectfully
- Keep 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 (KS) 2** at Abbotswood 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 their time at Abbotswood, 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/carers about online safety

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

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are learning in computing lessons and sites that they are using for home learning

If parents/carers 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/ DDSLs.

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 1 person or group by another person or group, where the relationship involves an imbalance of power.

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.

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/carers so 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 behaviour 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/ DDSLs will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff 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, DSL or DDSLs
- 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 co-operation

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 DSL/ DDSLs 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/carer 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/ DDSLs immediately, who will decide what to do next. The DSL/ DDSLs 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
- UKCCIS 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.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Abbotswood recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deep fakes', where AI is used to create images, audio or video hoaxes that look real. This includes deep fake pornography: pornographic content created using AI to include someone's likeness.

Abbotswood will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by Abbotswood pupils.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 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, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Pupils may bring mobile phones into school to use outside of school time; for example, to contact parents/ carers when they are walking to and from Abbotswood without an adult. They are not permitted to use mobile phones during school time.

'School time' includes:

- Lesson time
- Break and lunch time
- Clubs before or after school, or any other activities organised by the school

Pupils are expected to turn off their mobile phones and to keep them in their lockers. Abbotswood takes no responsibility for any mobile phones brought into school by pupils.

If a pupil is found to have used their mobile phone during school time, their phone will be confiscated by a member of staff and the pupil's parent/ carer will be informed. The mobile phone will be kept at the office and the pupil's parent/ carer will need to collect this at the end of the day.

If a pupil is found to have brought in a mobile device that is not a phone (for example, a tablet), this device will be confiscated by a member of staff and the pupil's parent carer will be informed. The mobile device will be kept at the office and the pupil's parent/ carer will need to collect this at the end of the school day.

If a pupil is found to have used their mobile phone, or a mobile device, in a way that breaks the school's behaviour, anti-bullying, or safeguarding policy, the consequences will follow those laid out in these policies.

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 13 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol). This is updated every 180 days in line with current industry recommendations.
- Using two-step authentication for accessing any areas where information about pupils is kept including emails, Google Drive, CPOMs and Arbor
- By using a school device that uses Google Drive to securely store files. Only staff issued with logins have access.
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software (supervised by the ICT Manager) on non-Chrome devices. Chrome has security built into it although this is under constant review to ensure that remains the case.
- Keeping operating systems up to date by always installing the latest updates

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

Staff must use their professional judgement if using their device for non-work related purposes and ensure that they always abide by the school's terms of acceptable use.

If staff have any concerns over the security of their device, they must seek advice from the IT Manager or Headteacher.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow, but not be limited to, this procedure:

- Discussion with the pupil about their misuse to explain to them what they have done. If needed, evidence (e.g. a screenshot) of the Impero alert will be shown. This will be done by the DSL or DDSL.
- Consequences, in line with the behaviour policy, will be followed.
- The class teacher will be informed

- The parents/ carers will be informed
- The incident will be logged

This list is not intended to be exhaustive. 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 code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. 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, staff meeting 'spotlights', 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, threatening, 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 up the risks
- 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 DDSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also regularly update their knowledge and skills on the subject of online safety.

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.

12. Monitoring arrangements

The DSL and DDSLs log behaviour and safeguarding issues related to online safety using CPOMs.

This policy will be reviewed every year by the DSL and ICT Manager. At every review, the policy will be shared with the governing board. As part of the review, the ICT Manager and DSL will use the 360 Safe review tool kit. They will also conduct 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.

Appendix 1: Abbotswood Technology Charter for Pupils

This technology charter outlines the expectations of acceptable use of ICT systems by pupils. This is shared every year with pupils who sign the charter. The charter is then referred to throughout the year.

Technology Charter

It Really Does Matter

Our computers are very safe but sometimes technology can be unsafe. It is important that we follow these rules to keep as safe as possible:

1. We will only use our own login details and not share passwords..
2. We will keep our personal information private.
3. We will check with an adult before...
    - using the internet
    - downloading anything
    - using a memory stick
    - printing
    - creating or deleting files
    - opening an attachment

4. We will respect and look after our technology by asking an adult before we unplug or plug in any devices.
5. We will use them in the way an adult has shown us.
6. We will leave our mobile electronic devices at home (unless we have permission from our teacher to bring them in).
7. If we bring a mobile phone into school and it is heard, it will be taken by an adult. The phone will then need to be collected by a parent or guardian. The school accepts NO responsibility for the loss, theft or damage of the phone.
8. We will only use school technology when we have permission to do so.
9. We will only use school technology for school activities – if we are not sure what these are, we will ask an adult.
10. We will respect copyright law.
11. We will tell an adult if we see something online that upsets us or makes us worried.
12. At break times, we are allowed to use computers if we have permission from an adult. We are only allowed to play educational games; such as, Times Tables Rock Stars. There will always be an adult with us when we are using school technology.

We are taught about how to be safe when using technology. The learning we do is updated every year.

Our teachers and LSAs are taught how to keep us safe online. Abbotswood aims to protect our personal information at all times.

Mr Pentland can see everything that we do online at Abbotswood. If we use technology in the wrong way, we may be stopped from using it.

Appendix 2: Abbotswood Technology Charter for Parents/ Carers

This technology charter outlines the expectations of acceptable use of ICT systems so that parents/ carers understand what is expected of pupils. This is shared at the start of each year with all parents/ carers so that they are aware.

Parent and Carer Technology Charter
It Really Does Matter

These rules help protect children and the school by describing acceptable use of technology. The school owns the computer network and can see anything pupils or staff do on it. People who use technology in school in the wrong way may be stopped from using it.

1. Children and staff must only use their own login
2. Children and staff will keep personal information private
3. Children and staff will check with a teacher/ICT technician before
    - using the internet
    - downloading
    - using a memory stick
    - printing
    - creating or deleting files
    - Using new software
4. Children and staff will respect school property and look after and maintain our technology. This includes not plugging or unplugging any devices and using them as instructed by their teachers or ICT Manager.
5. Children and staff understand that no children should bring any mobile electronic device into school.
6. Children and staff understand that no children should be bringing a mobile phone to school. However the school recognises that there may be a few children who travel to and from school independently and carry a mobile phone for safety purposes. In these instances;
    - If we see it or hear the phone in school, then we will take it from the child.
    - These confiscated phones will need to be collected by the parent or guardian from reception between 8am and 4pm.
    - The school accepts NO responsibility for loss, theft or damage and the office will not hold any devices for safe keeping
7. Children will only use school technology when they have permission to do so
8. Children will only use technology for school approved activities – if not sure what these are they will ask an adult/ICT Technician
9. Children and staff will respect copyright law
10. Children and staff will tell an adult/Designated Safeguarding Lead if they see something that upsets them online.

Abbotswood school has a secure network with a strong firewall, virus detection and monitoring in place. However, whilst we will take all reasonable precautions to ensure pupil's use of technology is always safe, we cannot guarantee this due to the pace of change in technology. We believe that following the guidelines above is the best way to be confident of children's safety whilst using our technology.

Sometimes children have approved access to technology in break times, at these times they are only permitted to use Times Tables Rock stars. ICT lessons are supervised by the children's teacher. Children are always supervised when using devices to go online.

Our school curriculum teaches our children about a range of safety measures when using technology. We update it to reflect changes in technology.

Staff are also subject to further guidance within our safeguarding policies.

Appendix 3: Abbotswood Technology Charter for Staff

This technology charter outlines the expectations of acceptable use of ICT systems for all staff. This is shared with all staff.

Staff Technology Charter

These rules help protect children and the school by describing acceptable use of technology. The school owns the computer network and can see anything pupils or staff do on it. People who use technology in school in the wrong way may be stopped from using it.

1. Staff will only use their own login and will keep devices 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). Passwords will be updated regularly.
2. Staff will make sure devices are locked if left inactive for a period of time.
3. Staff will use two-step authentication for accessing any areas where information about pupils is kept including emails, Google Drive, CPOMs and Arbor. Data will only be stored on Google Drive so the files can only be accessed by authorised personnel.
4. Staff will keep personal information private
5. Staff will check with the ICT Manager before
    - using a memory stick
    - using new software
6. Staff will respect school property and look after and maintain our technology. Staff must make sure that devices are not shared among family members or friends. Staff will make sure that they keep operating systems up to date by installing the latest updates (including anti-virus and anti-spyware software) as instructed by the ICT Manager or when they receive a reminder.
7. Staff will only use school technology when they have permission to do so.
8. Staff will use technology appropriately for activities that adhere to the school safeguarding policies and ethos. They will speak to SLT or the ICT Manager if they are unsure.
9. Staff will respect copyright law
10. School staff must take care to protect their privacy and protect themselves from the risk of allegations in relation to inappropriate relationships and cyberbullying linked to social media sites. Staff must not have any unauthorised contact or accept ‘friend’ requests through social media with any pupil (under 18 - including former pupils and/or those who attend other schools) unless they are family members.
11. Staff must exercise caution when having contact online through social media with parents so as not to compromise the school’s reputation or school information.

Abbotswood school has a secure network with a strong firewall, virus detection and monitoring in place. However, whilst we will take all reasonable precautions to ensure use of technology is always safe, we cannot guarantee this due to the pace of change in technology. We believe that following the guidelines above is the best way to be confident of staff and children’s safety whilst using our technology.

Staff are also subject to further guidance within our Safeguarding and Code of Conduct policies.

Abbotswood aims to be fully compliant with Data Protection and General Data Protection Regulation at all times.