Tillingbourne School Online Safety Policy

Adopted September 2025

Review September 2026

VISION:	AIM:	RIGHTS RESPECTING SCHOOLS (RRS)	Behaviour charter
At Tillingbourne we want children to: 1. Love Learning 2. Find their strengths and talents 3. Achieve more than they thought possible	**Children are successful at Tillingbourne School because they are:** • Aspirational • Responsible • Resilient • Curious • Confident • Caring	**FOCUS RIGHTS** 1. The right to learn 2. The right to be heard 3. The right to be me	**All children must be:** Ready Respectful Safe

Online safety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for **Behaviour Improvement, Remote Learning, Safeguarding, Anti-bullying, Staff Code of Conduct** and **Data.**

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

Using this policy

- The school will form an online safety committee consisting of the Online Safety Coordinator, Computing Curriculum Leader, ICT Support Technician, Headteacher/Safeguarding Lead (DSL) and Online Safety Governor. The committee will meet termly.
- The Online Safety Coordinator is Ben Stevenson.
- Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by staff and approved by governors.

- The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The online safety policy covers the use of all technology which can access the school network and the internet. This includes but is not limited to desktop computers, laptops, mobile phones, and tablets used on the school site. It also covers use of technology which facilitates electronic communication from school to beyond the bounds of the school site e.g. school email and remote access to the school system.

Managing access and security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school.

- The school Broadband is provided by B4RK.
- The age appropriate filtering is provided via PROTEX by E2BN. The filtering system is regularly checked (minimum fortnightly) to ensure that it is working, effective and reasonable.
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school networks will be controlled by **personal** passwords which are changed every 2 months.
- The security of school IT systems will be reviewed regularly by our ICT technician and in addition external auditors.
- The ICT technician who manages the filtering systems and monitors IT use will be supervised by senior management and have clear procedures for reporting issues.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

Monitoring

The following systems are in place to ensure that online use is monitored and this informs online safety policy:

- Physical monitoring of computers (and other devices) with online access
- Pro-active monitoring software (PROTEX by E2BN) which alerts the online safety committee of any inappropriate behaviour or potentially harmful material being accessed
- The Online Safety Log has evolved to the use of CPOMS. This will be used to report and track all online safety incidents and record what action has been taken to protect children and/or staff and inform online safety policy. This is a comprehensive system as it tracks online safety alongside all other safeguarding/behaviour concerns
- School will take all reasonable persuasions to ensure online safety for all users but recognises that incidents may occur inside and outside of the school which will need intervention. The school will ensure:

- That clear reporting reports are understood and followed by all members of the school community
- All members of the school community are made aware of the need to report online safety issues/incidents

Internet Use

In lessons where internet use is pre-planned it is best practice that pupils should be guided to sites checked as suitable for their use. Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites visited.

The school will provide an age-appropriate online safety curriculum (project evolve and be internet legends) that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. This is supported by our digital leaders.

Pupils are taught about online safety issues including the attached risks of sharing personal information. Pupils are taught to keep personal details which may identify them or their location private. In addition, key online safety messages are reinforced in assemblies and class activities and across the curriculum, pupils are taught to be critically aware of the content that they access online and are guided to validate the accuracy of information.

Many parents and carers have only a limited understanding on online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring of children's online behaviours. As a result of this, the school provides information and awareness to parents and carers through:

- curriculum activities
- the newsletter and website
- curriculum evenings
- high profile events e.g. Safer Internet Day

E-mail

- Pupils and staff may only use approved e-mail accounts on the school IT systems.
- All communication between staff and pupils or families will take place using school equipment and/or school accounts.
- Pupils only have access to email via dB Primary. This is a closed network which means that pupils are only able to email other members of the Tillingbourne School dB Primary network.
- dB Primary is a safe and secure platform which is monitored closely and has a comprehensive filtering system which flags all inappropriate content to members of staff. Pupils are also able to report inappropriate content using the whistle function.
- Where the dB email is opened up to allow for communication to those outside the network, this will be for a short period of time only and will be closely monitored.

- Staff to pupil email communication must only take place via the learning platform DB Primary.
- Where referring to pupils in emails, initials should be used in the subject heading.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known and you are expecting an attachment. Staff should contact the IT technician if they are in any doubt about a particular email.
- The school ensures that when a unit of work involves pupils emailing to external bodies safe practice is paramount and guides all communication.

Published content e.g. school website, Learning Platform (DB Primary)

- The contact details will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility of the website and will ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Written permission will be obtained from parents or carers before photographs, films featuring children or names of pupils are published on the school web site. Photographs are not accompanied by the child's name and only first names are published including in the weekly newsletter.
- If the school shares films or images which feature children for parents to view on platforms such as Youtube, these will be only be accessible through passwords via a private account. Permission will be sought from parents and access will be time bonded to 2 weeks. Parents will also be reminded to not share any of these images more widely.
- When using dB Primary the children can upload images including of themselves. This is a closed platform which is only accessible by staff and children

Use of social media including the school learning platform

- The school uses dB Primary as a safe platform for learning about social networking sites. Children do not have access to any other social networking sites in school. Children are educated on the safe use of social networking platforms through the curriculum and through their use of dB primary. This includes a whistle blowing function.
- Staff and pupils should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community.

- Where parents have taken photos during school events e.g. class assembly and Christmas play etc, parents will be asked to ensure that they do not share these photos on social media.

Remote learning including use of Zoom and Loom

Contact with pupils – own devices etc

Where a child needs to work from home, online learning may be provided.

Online learning will be accessed via dB Primary which is a safe and secure online learning platform.

Where staff are using online resources such as Oak Academy, they will ensure that the content is appropriate and will advise the children to avoid uploading their work to social media sites.

Where access to online devices is limited we will endeavour to support families by loaning laptops and chrome books. Families borrowing devices will sign an agreement with the school showing that they accept the responsibility of ensuring that their child is protected online by setting up parental controls through their broadband provider and through monitoring their access to the internet.

Use of personal online devices

Use of personal online devices in school – Pupils

- Pupils are not allowed to bring mobile phones or other personal online devices into school unless their parents have agreed with the child that this is necessary for activities before or after school. Any phone brought to school for this purpose must be handed to the class teacher at the start of the day and collected at the end of the day. The school does not take any responsibility for devices brought into school and parents are made aware of this.
- Pupils are not allowed to bring mobile phones or other online devices on school visits.
- Personally-owned mobile devices other than phones such as smart watches are not allowed to be brought into school by pupils. Basic fitbits can be worn into school as long as they are only used for telling the time and giving information about exercise.
- If a member of staff suspects a message, text or similar on a child's phone may contain inappropriate content it should not be opened. The DSL should be informed immediately. (See Safeguarding Policy for clarification of subsequent actions).

Use of personal online devices in school – Staff (see acceptable use policy for visitors including governors)

- Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode where possible unless it has a school-based purpose for example – caretaker role to set alarm for school gates or when taking a group to the forest school (see staff code of conduct).

- Mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Mobile phones may be taken outside by staff for use during outdoor learning sessions but are required to still follow policy.
- Staff will not take photographs or videos of children on personal devices such as mobile phones. Photos taken by staff and volunteers should be taken on school equipment; the personal equipment of staff/volunteers should not be used except as authorised by the trust/school and with appropriate consent. School cameras are available.
- If a member of staff breaches the school policy then disciplinary action may be taken as appropriate.
- Staff use of mobile phones during the school day will normally be limited to break-time, lunch break and after school and needs to be in an appropriate area of the school where children are not.
- Where mobile phones are used to access the internet within school, the school system must be used.
- Staff should ensure that their phones are protected with PIN/access codes in case of loss or theft.
- Staff should not send and receive texts during lesson times or staff meetings.
- Staff should never store parents' or pupils' telephone or contact details on their mobile phone, as this allows the possibility of inappropriate contact.
- Parents should not be given access to staff personal numbers. On school trips these should be redacted from the risk assessment.
- Staff should never send, or accept from anyone, texts or images that could be viewed as inappropriate.
- Personal equipment such as laptops and tablets may be used by staff to access the school IT systems provided their use complies with the online safety policy.
- Staff must not store images of pupils or pupil personal data on personal devices. Where photos are taken on pupils, this must be for educational purposes and must follow the relevant policies about sharing and using.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.
- When accessing online content at school, staff must ensure that they are using the school's wireless network.

Protecting personal data

- The school has a separate Data Protection Policy. It covers the use of biometrics in school, access to pupil and staff personal data on and off site, remote access to school systems.

Authorising access

- All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, ICT technicians and governors) must read this policy and sign to declare compliance with it before accessing the school IT systems.

- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- People not employed by the school must read and sign a Guest AUP before being given access to the internet via school equipment.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor LPAT can accept liability for the material accessed, or any consequences of internet access.

Handling online safety complaints

- Complaints of internet misuse will be dealt with according to the school behaviour policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the schools' behavior policy.
- Incidents involving online safety will be logged and tracked on CPOMS.

Communication of the Policy

To pupils

- Pupils need to agree to comply with the school's 'Online Safety Guidelines' in order to gain access to the school IT systems and to the internet. Online safety is repeated explicitly within the School Behaviour Code. Safe internet use is green behaviour.
- Pupils will be reminded about the content of the 'Online Safety Guidelines' as part of their online safety education.

To staff

- All staff will be shown where to access the online safety policy and its importance explained.
- All staff must sign and agree to comply with this policy in order to gain access to the school IT systems and to the internet.
- All staff will receive online safety training on an ongoing basis.

To parents

- Parents' and carers' will be updated with online safety updates in newsletters, and can access the policy through the school website.