Acceptable Use and Online Safety Policy

Author(s)	Mr M Haswell
Review body	Governing Body-Chair of Governors and Safeguarding Governor
Date of review	August 2026
Date of next review	August 2027
Website requirement	Yes
Inspection folder requirement	Yes

Significant amendments

Date	Amendment	Initials
15/8/25	Enhanced emphasis on the DSL's lead role in online safety, including understanding and reviewing filtering/monitoring systems (per KCSIE 2025).	MH
17/8/25	New sections on generative AI risks, deepfakes, financial extortion ('sextortion'), and latest trends (e.g., AI-generated CSAM, anonymous chat apps).	MH
25/8/25	Updated training requirements for staff, governors, and pupils on filtering/monitoring and online risks.	MH
27/8/25	Strengthened guidance on child-on-child abuse online, examining devices, and data protection in line with KCSIE and DfE standards.	MH
27/8/25	Integration of cross-curricular education using 'Teaching Online Safety in Schools' and 'Education for a Connected World'.	MH
27/8/25	Consulted the Model Policies for ISBA, LGFL and the Key with important updates.	MH

PRESTFELDE

Acceptable Use and Online Safety policy

Prestfelde School

September 2026

Acceptable Use and Online Safety Policy

Introduction

Prestfelde School recognizes that access to technology enhances learning, engagement, communication, and skill development for pupils and staff. We are committed to fostering 21st-century skills while prioritizing safeguarding. This policy outlines guidelines for technology use, ensuring a safe environment in line with KCSIE 2025, 'Teaching Online Safety in Schools', statutory RSHE guidance, and other statutory documents.

Online safety is integral to safeguarding and requires a whole-school, cross-curricular approach (incorporating the 4 Cs: content, contact, conduct, commerce). It sits alongside our Child Protection & Safeguarding Policy. Any online safety concerns must follow safeguarding procedures.

This is a living document, reviewed annually and amended as needed in response to school developments, local trends, or legislation.

Headmaster Mr Matty Thavenot	Email: head@prestfelde.co.uk Tel: 01743 245 400
Designated Safeguarding Lead (DSL) Mr Michael Haswell (Deputy Head Pastoral and SLT)	Email: mhaswell@prestfelde.co.uk Tel: 01743 245400 Mobile: 07915053721 (this number is to be used for emergency holiday contact or out of hours only)
Deputy Designated Safeguarding Lead (DDSL) Mr James Peakman (Assistant Head)	Email: jpeakman@prestfelde.co.uk Tel:01743 245400
Deputy Designated Safeguarding Lead (DDSL) Holly Keogh-Jones (Head of Boarding and Well-being)	Email: hjones@prestfelde.co.uk Tel: 01743 245400
Deputy Designated Safeguarding Lead (DDSL) Mr Edward Brittleton (Middle School and Assistant Housemaster)	Email: ebrittleton@prestfelde.co.uk Tel:01743 245400
Head of PSHE/RSE Mrs Emily Ratcliffe	Email: eratcliffe@prestfelde.co.uk Tel:01743 245400
Mental Health Lead Mrs Anna Price (SENDCo)	Email: aprice@prestfelde.co.uk Tel:01743 245400

Online Safety Lead Mr Michael Haswell (Deputy Head Pastoral and SLT)	Email: mhaswell@prestfelde.co.uk Tel: 01743 245400
Chair of Governors Mr Rex Sartain	Email: rsartain@prestfelde.co.uk Tel: 01743 245 400
Nominated Safeguarding Governor and Link Governor for Web Filtering Mr Rex Sartain	Email: rsartain@prestfelde.co.uk Tel: 01743 245 400
Network manager / other technical support	Email: semsley@prestfelde.co.uk Tel: 01743 245 400

This Acceptable Use Policy outlines the guidelines and behaviors that pupils are expected to follow when using technologies in school or when using their Device on the school site.

- The Prestfelde wireless network is intended for educational purposes.
- Devices brought into school are for the sole use of the individual child.
- All activity over the network or using school technologies will be monitored and retained.
- Access to online content via the network is restricted in accordance with our policies and regulations.
- Pupils are expected to follow the same rules for good behavior and respectful conduct online as offline.
- Misuse of school resources can result in disciplinary action.

Prestfelde makes a reasonable effort to ensure pupils' safety and security online but will not be held accountable for any harm or damages that result from use of school technologies.

Users of the Prestfelde network or other technologies are expected to alert the school immediately of any concerns for safety or security.

Acceptable Use Policy

1. Using Your Device at School

Devices are intended for use at school each day. In addition to teacher expectations for device use, you may use your device to access school messages, calendars, Microsoft Office (Including Teams and OneNote) and timetables.

2. Hot Spots and 4G

Pupils are not permitted to connect to the internet using a detected hot spot or 4G/5G account while at school.

These kinds of devices are not required by the school.

3. Charging Your Device's Battery

Devices must be brought to school each day in a fully charged condition. Pupils need to charge their devices each evening.

Keep in mind that this process can take up to 5 hours to fully charge a device depending on the percentage of battery life remaining.

Charging stations will be available in each form room, but pupils are only permitted to use these under exceptional circumstances.

4. Screensavers/Background photos

The lock screen and background of the Device should fall within what we would regard an acceptable image.

5. Photos and video

Taking photos or videos in class is prohibited unless a teacher expressly gives permission. Any breech of this will result in the camera and/or the device being restricted.

We expect pupils to use technology in a way that is safe, appropriate, careful, and kind. Don't try to get around technological protection measures; use good common sense and ask if you don't know or unsure.

6. Sound, Music

On *school-owned Devices:* pupils may not download music from any music sharing site unless directed by or with the permission of a teacher.

On all Devices: Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes.

7. Gaming

Pupils are NOT permitted to use gaming apps or websites during class time. Teachers always reserve the right to ask students to close their gaming app or to do random “flip checks” during instruction time.

8. Printing

Printing will be available with the device with teacher permission only. Pupils will be given information and instruction on printing with the device at school.

9.Saving Work

All pupils will save work on their school owned OneDrive account or inside their Class Team OneNote. Pupils should ensure that their OneDrive's are kept in good order.

Pupils will be taught good “housekeeping” skills to help manage their OneDrive effectively.

It is a pupils responsibility to ensure all their work is saved before logging off or exiting their application. If unsure, ask for help.

10. Network Connectivity

While we aim to keep Prestfelde’s network running as best we can, Prestfelde makes no guarantee that the school wireless network will be up and running 100% of the time.

11. Inspection

Pupils may be selected at random to provide their device for inspection and/or testing of web filtering. All device activity will be monitored by our Smoothwall web filter.

12. Web Access, including Wi-Fi

Prestfelde provides students with access to the Internet via our Prestfelde Wi-Fi. This include accessing web sites, resources, content, and online tools.

Pupils must use their own school credentials when logging onto Prestfelde Wi-Fi. A person’s access will be restricted in compliance with regulations and school policies. Web browsing may be monitored, and web activity records may be retained indefinitely.

Users are expected to respect that the web filter (Smoothwall) is a safety precaution and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn’t be, the user should follow Prestfelde protocol to alert a member of staff.

13. E-Mail and Teams chat.

Prestfelde will provide users with a school account for the purpose of school-related communication. This includes an E-Mail and a Teams account via Office 365. Availability and use may be restricted based on school policies.

When users are provided with these accounts, they should be used with care. Users should not send personal information, should not attempt to open files or follow links from unknown origin, should use appropriate language, and should only communicate with other people as allowed by Prestfelde policy or their teacher.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. E-Mail usage may be monitored and archived.

14. Collaborative Content

Recognizing the benefits collaboration brings to education, Prestfelde may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored, and users should be careful not to share personally-identifying information online.

15. Security

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin.

If you believe a computer or mobile device you are using might be infected with a virus, please alert IT. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

All Prestfelde devices will have Smartwater applied to them.

Whilst in school devices will remain on the child's desk when in use, during break or lunch times, devices will remain in the form room and doors will be locked. At the end of the day devices will be either taken home securely in their bag or stored in their form room locker to be charged and the room will be locked.

16. Senso

Senso is a safeguarding and security software that is installed on all school-owned IT equipment.

Senso provides us with full visibility of pupils' machines and uses key-word logging and live screen-capture to identify any possible threats.

Senso also allows us to view a pupil's screen as they are working, with the added protection of keyword, application, and web blocking. This can also be used to demonstrate work on the Class's interactive Whiteboard or Screen, so pupils must ensure that all content on screen is suitable for their current lesson.

Senso has been designed with the UK Government Prevent duty, UK Safer Internet Centre, the UK Department for Education's Keeping Children Safe in Education (KCSiE) guidance and with keyword and Illegal URL lists from the Internet Watch Foundation (IWF) all in mind.

Senso is able to detect violations and capture evidence of computer and internet misuse so that we can view and decide on any necessary action if required.

17. Internet Watch Foundation

The IWF is part of the UK Safer Internet Centre, working with Childnet International and the South West Grid for Learning to promote the safe and responsible use of technology.

Online Safety Policy

1. Aims

Prestfelde School aims to:

- Implement robust processes to ensure the online safety of pupils, staff, volunteers, and governors.
- Identify and support pupils at greater risk of online harm.
- Deliver an effective whole-school approach to online safety, empowering protection and education in technology use, including mobile/smart technology ('mobile phones').
- Establish clear mechanisms to identify, intervene in, and escalate incidents.

The 4 key categories of risk

Our approach addresses the 4 key categories of risk (KCSIE 2025):

- **Content**: Exposure to illegal/inappropriate/harmful content (e.g., pornography, misinformation, racism, self-harm).
- **Contact**: Harmful interactions (e.g., peer pressure, grooming, exploitation).
- **Conduct**: Behaviors causing harm (e.g., sharing explicit images, online bullying).
- **Commerce**: Risks like gambling, phishing, scams.

2. Legislation and guidance

This policy aligns with:

- KCSIE 2025.
- DfE's 'Teaching Online Safety in Schools' and 'Meeting Digital and Technology Standards'.
- Statutory RSHE guidance.
- Legislation including the Education Act 2011, Education and Inspections Act 2006, Data Protection Act 2018/UK GDPR, and Equality Act 2010.
- National Curriculum computing programmes of study.
- DfE guidance on preventing bullying, searching/screening/confiscation, and protecting children from radicalization.

It complies with our funding agreement and articles of association.

The policy also takes into account the National Curriculum computing programmes of study.

Current Online Safeguarding Trends

Over the past year at Prestfelde, we have noted increased device misuse, including unauthorized gaming, inappropriate photo/video capture, and access to harmful content via mobile networks bypassing filters. Nationally, trends include:

- Explosive growth in generative AI (GenAI), enabling deepfakes, AI 'girlfriends', and CSAM (illegal under UK law; see Internet Watch Foundation reports).
- Financial extortion ('sextortion'), especially affecting teenage boys.
- Over 50% of 3-12-year-olds using social media despite 13+ age limits, with fake ages exposing them to harm.
- Anonymous chat apps and platforms like TikTok/YouTube as news sources spreading misinformation.
- Parental filming of staff interactions posted online, risking community harm.

We address these through education, filtering, and parental engagement.

3. Roles and responsibilities

All staff must read Part 1 of KCSIE 2025; those working directly with children read Annex B.

3.1 The governing board

- Overall responsibility for policy implementation and monitoring.
- Ensure staff training includes online safety/filtering/monitoring.
- Review filtering/monitoring annually (per DfE standards); meet with DSL/IT to discuss.
- Ensure teaching adapts for vulnerable/SEND pupils.
- Adhere to staff AUP.
- The governing board 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).

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, 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

3.2 The Headmaster

- Ensures consistent implementation.
- Supports DSL in policy review and incident management.

3.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (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:

- This list is not intended to be exhaustive. Leads on online safety, understanding/reviewing filtering/monitoring systems.
- Works with headmaster/governors to update policy annually.
- Manages incidents, logs them (Appendix 5), and reports to police/agencies as needed.

- Provides updates/training; undertakes annual risk assessments.
- Liaises with external services; ensures remote learning safeguards.
- Providing regular reports on online safety in school to the headmaster and/or governing board

The DfE guidance “Keeping Children Safe in Education” states:

“The designated safeguarding lead should take lead responsibility for safeguarding and child protection (**including online safety**). This should be explicit in the role holder’s job description.” … Training should provide designated safeguarding leads with a good understanding of their own role, … so they … are able to understand the unique risks associated with **online safety** and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college.”

NOTE: It is important to emphasise that these online safety issues are safeguarding, not solely technical issues. Technology provides additional means for safeguarding issues to develop. Schools may choose to combine the role of Designated Safeguarding Lead (DSL) and Online Safety Lead. If the roles of the Designated Safeguarding Lead and the Online Safety Lead are not combined, it is suggested that they work closely in collaboration due to the safeguarding issues often related to online safety.

The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data [1]
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying.

3.4 The ICT Team

The ICT Team is responsible for:

- Implements security procedures, including filtering/monitoring (reviewed monthly).
- Conducts regular system checks; blocks dangerous sites.
- Reports incidents; ensures data protection/backup.
- Collaborates with DSL on strategic decisions; maintains documentation.
- Uses tools like Smoothwall, Senso, and LGfL solutions (e.g., Sophos, HomeProtect).
- Ensuring that the school’s ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

- 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

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
- 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 policy.

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 resource sheet – Childnet International

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).

3.8 Data Protection Officer (DPO)

- Ensures data sharing supports safeguarding without undue barriers (per KCSIE/UK GDPR).
- Monitors access to safeguarding data; aligns with retention schedules (e.g., until age 25+).

3.9 PSHE/RSHE/Computing Leads

- Embed online safety (e.g., consent, healthy relationships, AI risks) in curriculum.
- Assess pupil progress (e.g., via quizzes); collaborate for whole-school approach.

4. Educating pupils about online safety

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

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools must teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage 1 (Little Prestfelde)**, 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 (Years 3-5 Middle School)** 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 (Year 6)**, 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

In **Key Stage 3 (Senior School Years 6-8)**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly, and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact, and conduct, and know how to report concerns

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 or Firefly. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.) Report illegal material to police.

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. Form teachers will discuss cyber-bullying with their tutor groups.

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/leaflets 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 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 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

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete the material, or
- Retain it as evidence (of a possible criminal offence* or a breach of school discipline), and/or
- Report it to the police**

* If a staff member **believes** a device **may** contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this 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.

** Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence.

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, and governors are expected to sign an agreement regarding the acceptable use policy. Visitors will be expected to read and agree to the school's terms on acceptable use policy 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.

8. Pupils using devices in school

Pupils may bring educational laptops, iPads or Chrome books into school if they have properly connected to the network using their school credentials and have signed the acceptable use policy.

All devices are to be used with the supervision of teachers and Prestfelde staff during

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement. 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 12 characters, with a combination of upper and lower-case letters, numbers, and special characters (e.g., asterisk or currency symbol) It is also recommended to use the "three random words" method to create a secure complex password.
- 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
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always install the latest updates

Staff members must not use the device in any way which would violate the school's terms mentioned inside of the acceptable use policy.

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 the IT department.

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 6.3 Examining electronic devices. 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/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 which 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, 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 recognize 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 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. This will be via National 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 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 Deputy Head Pastoral (DSL) along with the ICT lead. At every review, the policy will be shared with the governing board. The review (such as the one available here) 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.

13. Artificial Intelligence (AI)

- GenAI (e.g., ChatGPT) prohibited on school devices without permission (per AI Policy).
- No input of personal/confidential data; be aware of errors/misinformation.

- Educate on risks (e.g., deepfakes, CSAM); treat AI bullying seriously.

14. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: EYFS and KS1 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:	

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:
  o I click on a website by mistake
  o I receive messages from people I don't know
  o I find anything that may upset or harm me or my friends
• Use school computers for schoolwork only
• 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 will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2, KS3 and KS4 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 usernames 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've 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 • Create, link to, or post any material that is pornographic, offensive, obscene, or otherwise inappropriate • 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 **Prestfelde School does not permit any child to bring a personal mobile phone or other personal electronic device into school outside of those aligned in our BYOD Policy.** **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 • Have images of children on my personal devices • 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 Team 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: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

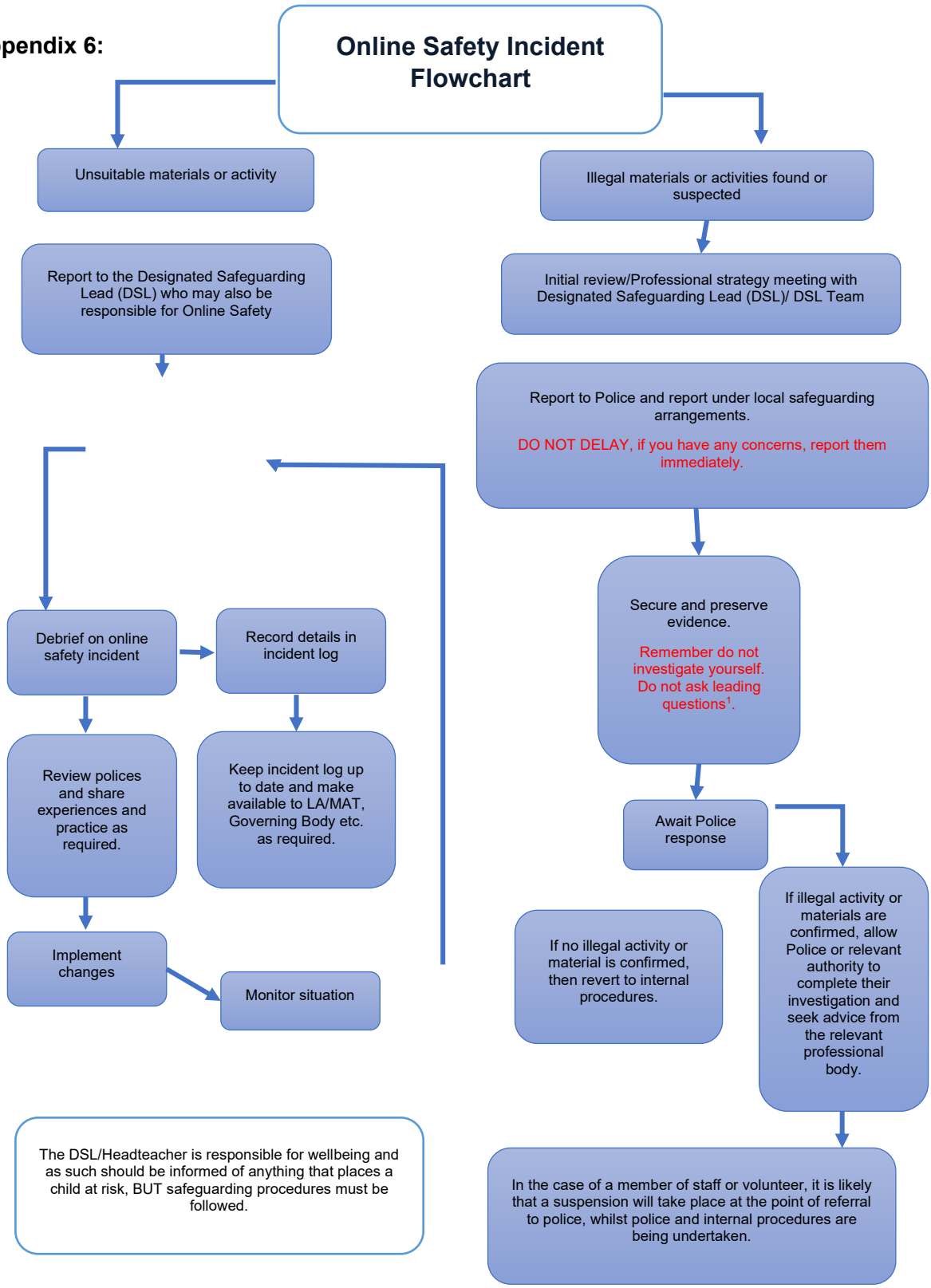
TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.

TERM	DEFINITION
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.

Appendix 5: 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 ways 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 6:


Online Safety Incident Flowchart
Unsuitable materials or activity
Illegal materials or activities found or suspected
Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ DSL Team
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
Await Police response
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.
If no illegal activity or material is confirmed, then revert to internal procedures.
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.
Implement changes
Monitor situation
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.