# Kew Green Preparatory School

# Online Safety Policy (including EYFS)

## Introduction

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can potentially place children, young people and adults in danger. Online safety covers issues relating to children and young people, as well as adults, and their safe use of the Internet, mobile phones and other electronic communication technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

KCSIE 2025 groups online safety risks into four areas: content, contact, conduct and commerce (sometimes referred to as contract). These are known as the 4 Cs of online safety. These are the cornerstones around which our Online Safety Policy is based. KCSIE 2025 clarifies the definition of content to include "being exposed to illegal, inappropriate or harmful

content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories."

This online safety policy sets out how the school plans to develop and establish its online safety approach and to identify core principles, which all members of the school community need to be aware of and understand. It works alongside the school's Safeguarding Policy to ensure all members of the school community are kept safe.

All online safety incidents should be reported to the School's Online Safety Officer who is Amy Kinross (Deputy Designated Safeguarding Lead); she has the lead responsibility for Online Safety.

Should a serious online safety incident take place, the Online Safety Officer will inform the DSL, Head and Data and Systems Manager. The procedure for investigating incidents is detailed in Section 9 below.

## Scope of the policy

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

The School will deal with online safety incidents in accordance with the procedure set out in this policy and associated school policies including the Safeguarding Policy, Behaviour, Rewards and Sanctions Policy, Acceptable Use Policies, Use of Mobile Devices, Data Protection Policy and Anti-bullying policy and will, where known, inform parents of incidents of inappropriate online safety behaviour that take place out of school.

## Roles and Responsibilities

### The Board of Directors

- The Board of Directors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Board receiving regular information about online safety incidents and monitoring reports.

- Theo Brehony is the named member of the Board of Directors with responsibility for Safeguarding, which includes online safety. This role involves meeting with the Online Safety Officer, reviewing the details of online safety incidents and reporting to relevant Board level meetings.
- Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, proprietors should ensure their school or college has appropriate filters and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Proprietors should consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks. The GSG IT department carries out a thorough process to vet and monitor appropriate sites via Sophos, with any inappropriate sites blocked and inappropriate use immediately flagged to DSL and Data and Systems Manager.
- Proprietors should ensure that roles and responsibilities to manage filtering and monitoring are applied, and that the school has effective monitoring strategies in place that meet their safeguarding needs. Proprietors should review the standards and discuss with IT staff and service providers what more needs to be done to support schools and colleges in meeting this standard of KCSIE.

The Head and the Senior Leadership Team

The Head has a duty of care for ensuring the safety of members of the school community, although the Online Safety Officer (DDSL) has lead responsibility for online safety.

The DSL, Head and SLT should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

The Online Safety Officer

The Online Safety Officer is responsible for:

- dealing with online safety incidents in their joint capacity as Online Safety Officer and Deputy Designated Safeguarding Lead (DDSL) in accordance with the DSL and the School's Safeguarding Policy;
- taking day-to-day responsibility for online safety issues and, in conjunction with the DSL, Head and Head of Computing, in establishing and reviewing the School's online safety policies / documents;
- ensuring that staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;
- in conjunction with the DSL and Head of Computing, arranging for training and advice to be provided for staff, parents and for pupils in liaison with the Head of Personal, Social, Health and Economic Education (PSHEE/PSED in EYFS). All staff should receive appropriate online safety training at induction, including an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring. The training should be regularly updated. In addition, all staff should receive safeguarding and child protection (including online safety)

updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively;

- liaising with School IT staff / the Local Authority where necessary;
- maintaining a log of online safety incidents on CPOMS to identify potential patterns of behaviour, to determine if any changes to this policy are required and to inform future online safety developments
- in conjunction with the DSL and Head of Computing, receiving reports of all online safety incidents and recording all investigations on CPOMS
- meeting with the Director with responsibility for online safety to discuss current issues, review incident logs and filtering;
- reporting to the DSL and SLT all serious online safety incidents.
- as part of the role of Deputy Designated Safeguarding Lead, assist the DSL to follow up any safeguarding issues that may arise from:
    - access to illegal or inappropriate materials;
    - inappropriate online contact with adults / strangers;
    - potential or actual incidents of grooming;
    - cyber-bullying (see the School's Anti-bullying policy).

The Data and Systems Manager

The Data and Systems Manager is responsible for ensuring that:

- the School's technical infrastructure is secure and is not open to misuse or malicious attack;
- only authorised users may access the networks and devices;
- the filtering policy is applied and updated on a regular basis, at least annually;
- the DDSL receives daily updates from FastVue Sophos, our system which updates filtering and monitoring real-time and provides a daily summary to the DDSL and Data Manager as well as immediate alerts to harmful contact, live-updated and checked regularly
- harmful and inappropriate content is blocked (without unreasonably impacting teaching and learning)
- investigations into any online safety incident in accordance with this policy are reported to the Online Safety Officer (see 'Responding to Incidents of Misuse' below);
- they keep up-to-date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant;
- the use of the School's network and devices is logged, and records can be provided and searched on request to ensure compliance with all the Acceptable Use Policies in order that any misuse / attempted misuse can be reported to the Online Safety Officer for investigation;
- the School's antivirus system definitions and web filter categories are updated automatically.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the School's Online Safety Policy and practices;

- they have read, understood and signed the Acceptable Use Policy Agreement for Staff (AUP for Staff) and Mobile Devices Policy;
- they report any suspected misuse or problem to the Online Safety Officer for investigation (see 'Responding to Incidents of Misuse' below);
- all digital communications by staff should be on a professional level and only carried out using official school systems;
- online safety issues are embedded in all aspects of the curriculum and other activities;
- pupils are helped to understand and follow this Online Safety Policy and the Acceptable Use Policy Agreement for Pupils;
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices;
- in lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and any filtering issues such as any unsuitable material that is found in internet searches should be reported immediately to the Data and Systems Manager and Online Safety Officer;
- any online material has been pre-checked, as far as practicable, before sharing with children. Websites, links, videos and audio should be high-quality and from reputable sources;
- parents and carers are aware of what their children are being asked to do online by KGPS, including the sites they will asked to access at home (for example, Atom Learning) and be clear who from the school (if anyone) their child is going to be interacting with online.

Pupils

- are responsible for using the School digital technology systems in accordance with the AUP for Pupils;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that this Policy covers their actions out of school, if related to their membership of the School.

Parents and Visitors

- Parents play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The School will take every opportunity to help parents understand these issues through parents' information evenings, newsletters, letters and information about national/local online safety campaigns/literature. Parents will be encouraged to support the School in promoting good online safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events as set out in the School's policy on Mobile Devices.

- It will be especially important for parents and carers to be aware of what their children are being asked to do online by the school, including which websites they are asked to visit

### Education of Pupils about online safety

Online safety should be a focus where technology is being used and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided and key online safety messages are reinforced as part of the Computing and PSHEE (PSED in EYFS) curriculum;
- Pupils are taught in all lessons to be critically aware of the content they access online and guided to validate the accuracy of information;
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Pupils are helped to understand the need for the AUP for Pupils and encouraged to adopt safe and responsible use both within and outside school;
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices;
- In lessons where internet use is pre-planned:
    - pupils are guided to sites checked as suitable for their use and any unsuitable material that is found in internet searches should be reported immediately to the Online Safety Officer and Data and Systems Manager;
    - Where pupils are allowed to search the internet, staff have pre-checked results, guide the process and are vigilant in monitoring the content of the websites the pupils visit.
- Teachers who are working with children in the Early Years Foundation should also refer to the following guidance: Safeguarding children and protecting professionals in early years settings: online safety considerations - GOV.UK (www.gov.uk).
  In particular:
  Children should be appropriately supervised when they are using mobile devices in the classroom.
  Staff should check all apps, websites and tools prior to using them with children, including checking the results of searches.
  Staff should use age-appropriate apps, websites and online tools with children.
  Staff should model safe practice when using technology with children.
  Staff should ensure data shared online is in accordance with the General Data Protection Regulations.
  *Full information regarding use of school and personal mobile devices can be found in our* ***Mobile Devices Policy****, including the below statement:*
  **Use of personal mobile devices is not permitted by members of KGPS staff within classrooms (including the Early Years classrooms). The use of personal mobile devices is not permitted by parents and volunteers. If a parent or other adult is visiting a classroom and they have their mobile device accessible, then they will be requested to put it away. Personal mobile devices should not be used for the taking of photographs or video footage of pupils.**

## Education and Training for Staff about online safety

All members of staff receive online safety training as part of their induction programme to ensure that they fully understand this online safety policy and the Accessible Use Policy for Staff.

Additional training is provided for all staff where appropriate as part of the INSET programme, including advice on cyber security and the use of AI. *An official AI Policy will follow in Autumn 2025.*

Prior to an official AI Policy, the school adheres to KCSIE 2025's guidance regarding AI. Generative artificial intelligence (Gen AI) refers to technology that can be used to create new content (e.g. text, code and images) based on the data the models have been trained on. Our school is aware of the potential benefits of using Gen AI, such as for reducing staff's workload and freeing up teachers' time. At the same time, our school is aware of the risks and dangers associated with using Gen AI. We will use the Department for Education's advice and guidance on using Gen AI in education to ensure we integrate Gen AI tools safely and with children's best interests at the centre. Safeguarding concerns that arise through an individual's use of artificial intelligence will be responded to in line with our safeguarding policies.

The Head of Computing monitors the provision of online safety teaching and updates the curriculum materials accordingly.

## Education and Training for Parents about online safety

An information workshop is organised for parents each year which is run either by the Head of Computing, Online Safety Officer or by organisations that specialise in online safety, and provide advice about access to the internet, online gaming, social media and the effects of screen time upon sleep.

Where a specific issue or concern relating to online safety has been brought to the School's attention, information and advice will be sent to parents via email or letter.

## Good practice in the use of communication technologies

KGPS is aware of the potential negative impact of screentime on the development of our pupils and we therefore ensure screen time is limited and only used to further support and enrich teaching and learning.

When using communication technologies, the School considers the following as good practice:

- The official School email service may be regarded as safe and secure. Staff and pupils should therefore use only the School email service via Office 365 to communicate with others when in school, or on school systems (e.g. by remote access);
- Users in receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature must not respond to any such communication and must immediately report it, but not delete the messages, to the Online Safety Officer and/or to the Head;

- Any digital communication between staff and pupils or parents must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications;
- If it is necessary to communicate via the school system with individual pupils, a parent of the pupil concerned and a member of the Senior Leadership Team should be copied in (exception will be made if the School enters Remote Learning);
- Pupils are provided with individual school email addresses for educational use from Year 3 upwards (all pupils are assigned an Office 365 account in order to access Microsoft Teams, but Lower School accounts are accessed by parents);
- Pupils are taught about online safety issues, such as the risks attached to the sharing of personal details. They are taught strategies to deal with inappropriate communications and reminded of the need to communicate appropriately when using digital technologies;
- Personal information should not be posted on the School website and only official email addresses should be used to identify members of staff.

### Unsuitable / Inappropriate Activities

The School believes that certain activities identified in the Acceptable Use Policies would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems.

Users shall not visit Internet sites, make, post, download, upload, transfer data, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images - the making, production, distribution of indecent images of children. Contrary to The Protection of Children Act 1978;
- Grooming, incitement, arrangement or facilitation of sexual acts against children. Contrary to the Sexual Offences Act 2003;
- Criminally racist material in UK - to stir up religious hatred (or hatred on the grounds of sexual orientation. Contrary to the Public Order Act 1986;
- Statements or images that are intended to radicalise people or in any other way endorse, condone or incite extremist or terrorist activity;
- Pornography;
- Promotion of any kind of discrimination;
- Threatening behaviour, including promotion of physical violence or mental harm; or
- Any other information which breaches the ethos of the School or brings the integrity of the School into disrepute.

Furthermore, the following is prohibited as part of the Acceptable Use Policies:

- Using school systems to run a private business;
- Using systems, applications, websites or other mechanisms that bypass deliberately the filtering or other safeguards employed by the School;
- Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords);

- Infringing copyright;
- Creating or propagating computer viruses or other harmful files;
- Unfair usage (downloading/uploading large files that hinder others in their use of the Internet);
- Online gaming (other than as part of the school curriculum);
- Online gambling

## Responding to incidents of Misuse

Reports of misuse may come from staff, pupils, parents or outside the School community. However, the incident is reported or discovered, the course of action is dependent on whether there is any suspicion that the misuse is in any way illegal.

Illegal Incidents

If anyone suspects that access has been attempted to any web site or materials are found on any electronic device containing:

- child abuse images;
- criminally racist material;
- statements or information intended to radicalize people or incite terrorist activity;
- incidents of online 'grooming' behaviour;
- material that breaches the Obscene Publications Act;
- indecent or explicit images of children, including sexting; or
- any other suspected illegal activity,

they must report all concerns, allegations, complaints or suspicions to the Head or Online Safety Officer unless that person is the subject of the concern.

All concerns, allegations, complaints or suspicions about:

- the Head should be reported to the Director with responsibility for Safeguarding (Theo Brehony)
- the Online Safety Officer should be reported to the Head;
- the Director with responsibility for Safeguarding should be made to the LADO (see Safeguarding Policy for contact details for the LADO).

For any substantial safeguarding concerns of a potentially illegal nature, the Online Safety Officer as DSL will immediately act in accordance with the School's Safeguarding Policy, including reporting the concerns to Children's Social Care and the

Police. If an allegation is made against a member of staff, the following will also be involved; Police, DBS, LADO or other external agency as appropriate.

If anyone is concerned about any IT illegal activity of a member of staff, pupil or parent (such as copyright theft, fraud, or unlicensed software), they should report this to the Online Safety Officer, who will inform the Head and also the Data and Systems Manager, who will in turn investigate using activity logs.

If a member of staff is concerned that issues raised are still not being addressed they should raise these in accordance with the School's Whistleblowing Policy and Procedure.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse of IT equipment or services.

- Reports by members of staff of online safety incidents which do not raise safeguarding concerns or appear to suggest illegal activity should be reported in the first instance to the Online Safety Officer.
- Misuse of IT equipment or services by members of staff, pupils or visitors should be reported to the Online Safety Officer.
- Misuse detected by the Data and Systems Manager will be investigated on discovery and then referred to the Online Safety Officer.

If any such misuse has caused, or is suspected to have caused, a data breach, this should be reported to the Data and Systems Manager who will investigate in line with the School's Privacy Policy.

### Investigating Incidents by the Online Safety Officer

- The Online Safety Officer will evaluate the report to determine the appropriate response.
- If necessary, the Online Safety Officer will initiate an investigation and request the Data and Systems Manager to investigate to establish, capture and preserve any relevant data or other evidence as set out below.
- Where appropriate, the Online Safety Officer will respond in accordance with the disciplinary procedures set out in the School's Behaviour Policy (for pupils) and Disciplinary Policy and Procedures (for staff).
- The Online Safety Officer will only examine the contents of personal devices not owned by the School in accordance with the procedures set out in the relevant Behaviour Policy.

### Investigating Incidents by the Data and Systems Manager

Where instructed by the Online Safety Officer, the Head, the Director with responsibility for Safeguarding, the DSL, the police or other appropriate external agency, the Data and Systems Manager will investigate as follows:

- Examination will be made of all technical logs;
- Detailed examination of firewall, filter systems, other will be undertaken;
- Remote examination of the School's desktops and laptops will be made. This is only possible where the computer is turned on and connected to the School network;
- Examination of relevant School emails, (including sent and deleted) will be made;

The investigation should be conducted using a designated computer in the IT Department. There should be two senior members of staff involved in this process, ideally the Data and Systems Manager and the Online Safety Officer. It is

important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

- A record of the URL of any site containing the alleged misuse will be made describing the nature of the content causing concern and unsuitable materials will be copied. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the report (except in the case of images of child sexual abuse or any other indecent images of children– see below)
- Once this has been completed and fully investigated, the Data and Systems Manager will report to the Online Safety Officer who will judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures in accordance with the School's Behaviour and Anti-bullying Policies
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
    - If the security of personal data has been compromised, consideration of whether a report to the Information Commissioner's Office is appropriate.
- If content being reviewed includes images of child abuse then the monitoring will be halted, the Online Safety Officer (in their capacity as DDSL), the DSL and the Head will be informed and the computer in question will be isolated as best we can. The matter will then be referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour;
    - the sending of obscene materials to a child, including those produced by children (sexting);
    - adult material which potentially breaches the Obscene Publications Act;
    - criminally racist material;
    - other criminal conduct, activity or materials.

It is important that all of the above steps are taken as they will provide an evidence trail for the School and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed written report should be retained for evidence and reference purposes.

- Under the direction of the appropriate authority, unsuitable materials will be deleted from the storage, mailboxes or computers in accordance with the procedures set out in the relevant Behaviour Policy.

### Sharing Nudes and Semi-Nudes (updated March 2024):

In the latest advice for education settings (UKCIS, 2024), this is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. Nudes and semi-nudes can be shared online via social media, gaming platforms, chat apps, forums, or involve sharing between devices using offline services. Alternative terms used by children and young people may include 'dick pics' or 'pics'. The motivations for taking and sharing nude and semi-nudes are not always sexually or criminally motivated.

This advice does not apply to adults sharing nudes or semi-nudes of under 18-year olds. This is a form of child sexual abuse and must be referred to the police as a matter of urgency.

The school follows government guidance when dealing with these such incidents; short-form procedure is detailed here.

The DSL must be informed immediately. A staff member will **never** view, copy, print, share, store or save the imagery, or ask a child to share or download – this is illegal. In exceptional circumstances, it may be necessary for the DSL (or equivalent) only to view the image to safeguard the child or young person. That decision should be based on the professional judgement of the DSL (or equivalent).

### Sanctions

- It is more likely that the School will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner.

- Incidents of misuse by pupils will be dealt with through disciplinary procedures set out in the School's Behaviour, Rewards and Sanctions and Anti-bullying Policies.

- Incidents of misuse by members of staff will be dealt with through disciplinary procedures set out in the Disciplinary Policy and Procedures.

**Written by:** Amy Kinross (DDSL), September 2022
**Last Reviewed:** Amy Kinross (DDSL), September 2025
**Next review:** September 2026