ICKWORTH PARK PRIMARY SCHOOL

Online Safety and Acceptable Use Policy

DATE ADOPTED / REVIEWED	Autumn 2025
PRINT NAME	
SIGNED	
DATE	
DUE FOR NEXT REVIEW	Autumn 2027
COMMITTEE TO APPROVE	Full Governing Body

1. **Aims**

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:
Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
Relationships and sex education – (under review and development)
Searching, screening and confiscation.

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

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

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
The governor who oversees online safety is our safeguarding governor.
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)

3.2 The headteacher

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

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) Headteacher and Deputy Headteacher are set out in our child protection and safeguarding policy.
The Head Teacher takes lead responsibility for online safety in school, in particular:

- In ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the IT Support supplier, computing subject leader and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on CPOMs and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs. This is included in the staff induction packs.
- Liaising with other agencies and/or external services if necessary
- Regular reports on online safety in school are provided to the governing board
- Liaise with IT technicians to put in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Liaise with IT technicians to ensure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Liaise with IT technicians to conduct a full security check and monitoring the school's ICT systems each visit (Fortnightly in school term only).
- Liaise with IT technicians to ensure to block access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

3.4 The IT Support supplier

The IT Support supplier is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's IT systems on a regular basis (agreed in contract)
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

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 IT 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 safeguarding team to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet (appendices 1 and 2)

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
- National Online Safety guides
- Parent factsheet - Childnet International
- National Online Safety guides (weekly guides sent out on Class Dojo)
- Our school website's section 'Online Safety'

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.
In **Key Stage 1**, pupils will be taught to:

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

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

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

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

- *That people sometimes behave differently online, including by pretending to be someone they are not.*
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*
- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*
- *How information and data is shared and used online*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*
- *That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners*
- *That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail*
- *How information and data is generated, collected, shared and used online*
- *How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours*

The safe use of social media and the internet will also be covered in other subjects where relevant.
The school may use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

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 Class Dojo messaging facility. This policy will also be shared with parents and on our website.
If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.
Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

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

6.2 Preventing and addressing cyber-bullying

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

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

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).

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

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

6.3 Examining electronic devices

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

Any searching of pupils will be carried out in line with the DfE's latest guidance on Searching, screening and confiscation.
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 of the school's IT systems and the internet (appendices 1 -3). All visitors will be expected to read various school policies as required.

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

- No user shall access (e.g. read, write, modify, delete, copy, move) another user's personal electronic documents (including email) without the owner's permission or as allowed by this policy or by law, other than the monitoring of acceptable use by school leaders.
- Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources. They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.
- Users are required to protect their password and not share their account details with others for their use, nor utilise another user account or misrepresent their identity for any reason. Users must not under any circumstances reveal their password to anyone else.
- Users must not load or download software or Apps on any device without the authorisation of the Headteacher. Periodic audits of software and Apps will be undertaken.
- Users must take care to store sensitive information, e.g. pupil data safely and to keep it password protected, on all school systems, including laptops.
- Network connected devices must have school approved anti-virus software installed and activated. Users may not turn off anti-virus software. All users of ICT resources have the responsibility to take precautions to prevent the initial occurrence and subsequent spreading of a computer virus. No one may knowingly create, install, run, or distribute any malicious code (e.g. viruses, Trojans, worms) or another destructive program on any ICT resource.
- Ensure that all personal storage devices (i.e. memory sticks/portable hard drives) which are utilised by staff members to hold sensitive information are encrypted or password protected with either fingerprint technology or 6-digit passcode lock in the event of loss or theft.
- Websites should not be created on school equipment without the written permission of the Headteacher.
- All users sign an Acceptable Use Statement to show that they agree with and accept the agreement for staff using non-personal equipment, within and beyond the school. By logging on to ICT systems, users agree to abide by this policy.
- Users may access school emails via personal mobile devices (i.e. iPad or mobile phone) providing the device is password protected (i.e. face recognition, fingerprint technology or passcode lock).

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

Staff/Adults (Online safety)

- All users are expected to act in a responsible manner, with the clear understanding that all information may be accessible to the public and under the Freedom of Information Act 2000. Privacy and confidentiality are in accordance with the current Data Protection legislation, the Human Rights Act 1998 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. The County Council or school may record or inspect any information transmitted through or stored in its computers, including e-mail communications and individual login sessions, without notice when:
    - There is reasonable cause to believe the user has violated or is violating this policy, any guidelines or procedures established to implement this policy.
    - An account appears to be engaged in unusual or unusually excessive activity
    - It is necessary to do so to protect the integrity, security, or functionality of ICT resources or to protect the County Council or its partners from liability.
    - Establishing the existence of facts relevant to the business.
    - Ascertaining or demonstrating standards which ought to be achieved by those using the ICT facilities.
    - Preventing or detecting crime
    - Investigating or detecting unauthorised use of ICT facilities
    - Ensuring effective operation of ICT facilities
    - Determining if communications are relevant to the business (for example, in the last resort where an employee is off sick or on holiday and business continuity is threatened)
    - It is otherwise permitted or required by law.
    - In any instances where a child accesses inappropriate web pages or other internet media (i.e. inappropriate for the child's age) the incident is to be recorded on CPOMS.
- Care must also be taken not to breach another person's copyright, trademark or design, nor to publish any defamatory content. No one may use ICT resources in violation of license agreements, copyrights, contracts or national laws, or the Standing Orders, policies, rules or regulations of the school or the County Council.

All staff and adults in school should:

- Know who the Online Safety Lead and Designated Safeguarding Lead is so that any misuse or incidents can be reported which involve a child.
- Be up-to-date with online safety knowledge appropriate for the age group and reinforce through the curriculum.
- Be familiar with the Behaviour, Anti-bullying and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately. If a procedure is unknown, they will refer to the Headteacher/Designated Safeguarding Lead immediately, who should then follow the Managing Allegations Procedure, where appropriate.

- Alert the Online Safety Lead of any new issues and risks that may need to be included within policies and procedures.
- Not use ICT resources to transmit abusive, threatening, or harassing material, chain letters, spam, or communications prohibited by law. No one may abuse the policies of any newsgroups, mailing lists, and other public forums through which they participate from a school account. The following content **SHOULD NOT** be created or accessed on ICT equipment at any time:
  - Pornography and "top-shelf" adult content
  - Material that gratuitously displays images of violence, injury or death
  - Material that is likely to lead to the harassment of others
  - Material that promotes intolerance or discrimination on grounds of race, sex, disability, sexual orientation, religion or age
  - Material relating to criminal activity, for example buying and selling illegal drugs
  - Material relating to any other unlawful activity e.g. breach of copyright
  - Material that may generate security risks and encourage computer misuse

(It is possible to access or be directed to unacceptable Internet sites by accident. These can be embarrassing and such sites can be difficult to get out of. If staff have accessed unacceptable content or are in receipt of unacceptable material via email, they should inform the Headteacher. This will avoid problems later when monitoring systems are alerted to the content.)

- Ensure that children are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Children should know what to do in the event of an incident.
- Report accidental access to inappropriate materials to the Online Safety Lead and or control this with the Local Control options via your broadband connection.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies using the SCC incident reporting procedure in the same way as for other non-physical assaults.

To maintain a secure and controlled online environment, all staff and visitors requiring access to the school's guest Wi-Fi must sign the Acceptable Use Policy (AUP) form. This ensures that all users are aware of and agree to comply with our internet usage guidelines.

In order to maintain a secure and supportive online environment, it is sometimes necessary for the Online Safety Lead and the Computing Lead to conduct further investigations into issues identified through routine monitoring and filtering checks. This process ensures that any potential risks or breaches are thoroughly examined and addressed promptly, safeguarding the well-being and privacy of all users.

Additionally, when dealing with any reports or investigations related to online safety, we are committed to maintaining the highest level of confidentiality, ensuring that all information is handled with discretion and respect for privacy.

Digital Images

Staff have access to cameras, iPads, web cams and scanners. There may be instances when staff use their own photographic equipment, to take a high-quality image. This requires prior agreement with the head teacher and the relevant form completed and signed. These images must be stored to a central place e.g. – staff pool, admin server or encrypted USB within a few days and the original photos deleted from personal equipment. Once removed, the agreement form should be signed to confirm deletion and signed off by the head teacher. Images of children should be stored carefully in accordance with photo permission forms:

- as a record of significant events in the life of the school;
- to display and share in the school and educational communities;

Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a school website. Photographs should only ever include the child’s first name although safeguarding guidance states either a child’s name or a photograph but not both. Group photographs are preferable to individual children and should not be of any compromising positions or in inappropriate clothing, e.g. gym kit. It is current practice by external media such as local and national newspapers to include the full name of children in their publications. Photographs of children should only be used after permission has been given by a parent/carer.

Video-Conferencing and Webcams

The use of webcams to video-conference will be via a filtered service. Publicly accessible webcams are not used in school. Taking images via a webcam should follow the same procedures as taking images with a digital camera. Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school. This process should always be supervised by a member of staff and a record of dates, times and participants held by the school. Children need to tell an adult immediately of any inappropriate use by another child or adult. (This will be part of the Acceptable Use Agreement).

Managing Social Networking and Other Web Technologies

The school does not promote use of social networking sites within the curriculum, we teach children about such uses of technology through online safety education.

Social networking outside of work hours, on non-school-issue equipment, is the personal choice of all staff but is not recommended. Owing to the public nature of such websites, it is advisable for staff and governors to consider the possible implications of participation. The following advice should be considered if involved in social networking:

- Staff and governors should not engage in personal online contact with students outside of authorised school systems.
- Considering the COVID 19 pandemic, for exceptional remote learning circumstances when making welfare checks with pupils, home phones/personal mobiles must be set so that caller identity is blocked before making calls.
- Staff and governors should not comment on issues relating to school, on any social networking site. This includes for example, liking a comment.
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by students).
- Social networking is not used for communicating with students, even for professional purposes.
- Personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove

details from search results and turn off public visibility. Staff should ensure that full privacy settings are in place.
- Staff should not give out home or mobile telephone numbers or undertake instant messaging with pupils or parents.

Filtering

Our broadband internet service has a filter system which is set at an age appropriate level so that inappropriate content is filtered and tools are appropriate to the age of the child. All filtering is controlled via an approved DfE provider and for which an annual subscription is paid. Local controls enable access to specific websites and provides the option to add to a 'restricted list'. Children are directed to use specific child friendly search engines and should only use a full search engine, e.g. Google, with adult supervision.

Mobile phone communication and instant messaging

- Staff are advised not to give their home or mobile telephone number to pupils or parents/carers. Mobile phone communication should be used sparingly and only when deemed necessary.
- Photographs and videos of pupils should not be taken with mobile phones prior to permission form being completed and signed by the head teacher.
- Staff are advised not to make use of pupils' mobile phone numbers either to make or receive phone calls or to send to or receive from pupils' text messages other than for approved school business.
- Staff should only communicate electronically with pupils from school accounts on approved school business e.g. school work.
- Staff should not enter instant messaging communications with pupils.
- Staff should not make or accept friend requests from pupils on any social media platforms.

Children and Parents

Children are expected to use the internet and other technologies within school including downloading or printing of any materials in a responsible way as taught by the teachers. Each child receives a copy of the Acceptable Use Agreement on first-time entry to the school and when moving from Key Stage 1 to Key Stage 2. This is read with the parent/carer, signed and returned to school. The agreements are there for children to understand what is expected of their behaviour and attitude when using the internet and other technology. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

It is hoped that parents/carers will explain and discuss the agreement with their child so that it is clearly understood and accepted. This is also intended to provide support and information to parents/carers when children may be using the Internet beyond school. We keep a record of the signed forms.

The school promotes a positive attitude to using the internet and we want parents to support their child's learning and understanding of how to use online technologies safely and responsibly. We do this by publicising online safety on the school website and by teaching children how to agree rules for use of the Internet.

If a child **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window. Where a child feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child deliberately misusing online technologies should also be addressed by the establishment.

Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

The Curriculum and Tools for Learning

We teach children how to use the Internet safely and responsibly. They are also taught, through Computing and/or PSHE lessons, how to research information, explore concepts and communicate effectively to further learning. The following concepts, skills and competencies are taught by the time they leave the school.

- Internet literacy.
- Making good judgements about websites and e-mails received.
- Knowledge of risks such as viruses and opening mail from a stranger.
- Access to resources that outline how to be safe and responsible when using any online technologies.
- File sharing and downloading illegal content.
- Uploading information – know what is safe to upload and not upload personal information.
- Where to go for advice and how to report abuse.

These skills and competencies are taught within the national curriculum so that children have the security to explore how online technologies can be used effectively, but in a safe and responsible manner. Children should know how to deal with any incidents with confidence, as we adopt the ‘never blame the child for accidentally accessing inappropriate materials’ culture, in the event that they have accidentally accessed something.

Personal safety – ensuring information uploaded to web sites and e-mailed to other people does not include any personal information such as:

- Full name (first name is acceptable, without a photograph).
- Address.
- Telephone number.
- E-mail address.
- School Clubs attended and where.
- Age or DOB.
- Names of parents.
- Routes to and from school.
- Identifying information, e.g. I am number 8 in the school Football Team.

Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that would also be acceptable in ‘real life’. Parents/carers should monitor the content of photographs uploaded.

Pupils with Additional Learning Needs

The school strives to provide access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each pupil. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of online safety awareness sessions and internet access.

Websites and Class Dojo

The uploading of images to the school website or Class Dojo website/app, should be subject to the same acceptable agreement as uploading to any personal online space. Permission ought to be sought from the parent/carer prior to the uploading of any images. Settings should consider which information is relevant to share with the public on a website and use secure areas for information pertaining to specific audiences.

If a member of staff finds themselves or another adult on an external website, such as ‘Rate My Teacher’, as a victim, schools are encouraged to report incidents to the Headteacher and unions, using the reporting procedures for monitoring.

8. Staff, visitors and pupils using mobile devices in school

Using personal devices

- Personal data accessed by staff on their own devices must be kept secure to avoid a data breach and to remain compliant with GDPR. Access to personal data via staff email is permitted using a personal mobile device, providing the device is password protected (i.e. face recognition, fingerprint technology or passcode lock).
- Personal data must not be saved onto personal mobile devices or any insecure public online file hosting and sharing services. Where access is required to school files, this must be via a staff laptop where protection is achieved through the Firewall and VPN (Virtual Private Network).
- Personal mobile devices used to access staff emails must not be shared with other family members or friends.

There is a separate policy about the use of mobile phones in school. This policy applies to staff and other adults, and to the use of pupils’ mobile phones.
Although we do not expect pupils to bring mobile phones to school, we recognise some of our Year 5 and Year 6 pupils will be travelling to and from school independently so parents may wish them to bring one. There is a form for parents to sign to give permission for their child to bring a phone to school, [Appendix 1 of Mobile Phones Policy].

If the child brings a phone it must be switched off on arrival at the school site. It must be handed in at the start of the school day and will be stored securely until the end of the school day. The pupil is responsible for collecting the phone at 3.20pm and it must not be switched on again until they are leaving the school site. They may not be used during after school clubs and activities. Phones may not be stored in coats, bags or lockers.

Pupils must adhere to the school’s acceptable use agreement for mobile phone use [Appendix 1 of Mobile Phones Policy].

9. Staff using work devices outside school.

During normal operations, ICT resources are to be used for business purposes only. Staff who have been given the use of a school laptop or iPad and will be removing it from the premises will be expected to sign for its use on receipt. Staff must follow authorised procedures when relocating ICT equipment or taking mobile devices offsite. The school permits limited personal use of ICT facilities by authorised users. Staff may use school equipment for authorised business use under the following conditions:

- Personal use must be in the user's own time and must not impact upon work efficiency or costs.
- The level of use must be reasonable and not detrimental to the main purpose for which facilities are provided.
- Personal use must not be of a commercial or profit-making nature.
- Personal use must not be of a nature that competes with the business of the school or conflicts with an employee's obligations.
- Personal use of the Internet must not involve attempting to access the categories of content described above.
- Passwords must be protected and account details must not be shared.

Please also see our ICT and Internet Use, Mobile phones and Wearable Technology Policies.

10. How the school will respond to issues of misuse

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

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff 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.

Managing Allegations:
Allegations made against a member of staff should be reported to the Designated Safeguarding Lead (DSL) for safeguarding within the school immediately. In the event of an allegation being made against a Headteacher, the Chair of Governors should be notified immediately.

Local Authority Designated Officer (LADO)
The local authority has designated officers who are involved in the management and oversight of individual cases where there are allegations against an adult in a position of trust. They provide advice and guidance to all of the above agencies and services, and monitor the progress of the case to ensure all matters are dealt with as

quickly as possible, consistent with a thorough and fair process. In addition to this they liaise with the police and other agencies.

11. Training

All new staff members will receive training 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).
The DSL and deputy will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in CPOMS.
This policy will be reviewed every year, or sooner should KCSiE or other developments dictate, by the Headteacher. At every review, the policy will be shared with the staff and the governing board.

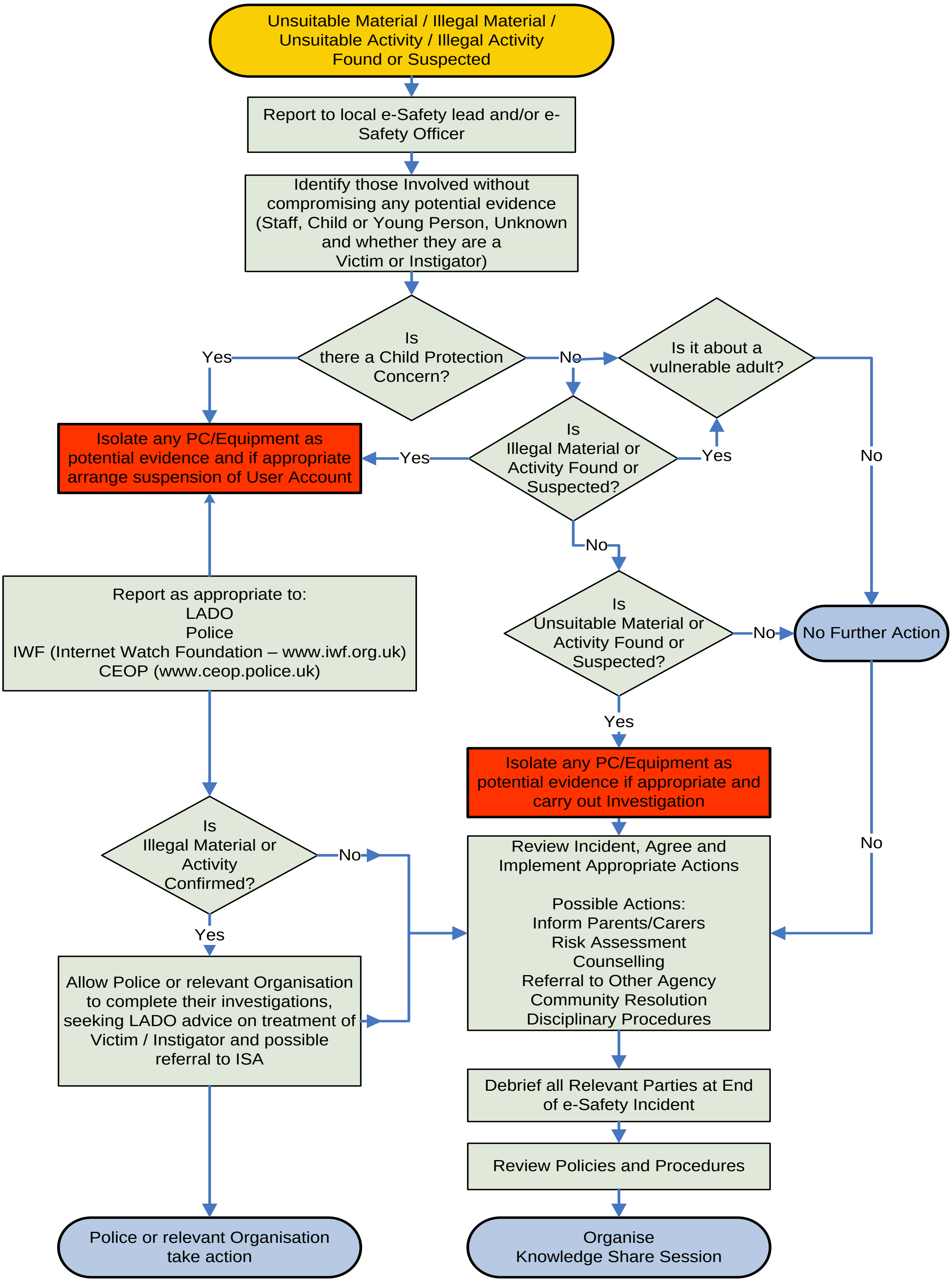
13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Keeping Children Safe in Education 2022 – Annex C safety deals specifically Online Safety
- Working Together to Safeguard Children 2019
- Mobile Phone and Wearable Technology Policy
- Online Safety policy All Saints Trust
- Whistleblowing Policy
- Behaviour Policy
- Staff Code of Conduct Policy
- Guidance on Safer Working Practice 2020
- Teaching Online safety in Schools DfE January 2023

- Data protection policy and privacy notices
- Complaints procedure
- Staff Handbook

Figure 1: Online Safety Flow Chart



Unsuitable Material / Illegal Material / Unsuitable Activity / Illegal Activity Found or Suspected
Report to local e-Safety lead and/or e-Safety Officer
Identify those Involved without compromising any potential evidence (Staff, Child or Young Person, Unknown and whether they are a Victim or Instigator)
Is there a Child Protection Concern?
Yes
No
Is it about a vulnerable adult?
Isolate any PC/Equipment as potential evidence and if appropriate arrange suspension of User Account
Yes
Is Illegal Material or Activity Found or Suspected?
Yes
No
No
Report as appropriate to: LADO Police IWF (Internet Watch Foundation – www.iwf.org.uk) CEOP (www.ceop.police.uk)
Is Unsuitable Material or Activity Found or Suspected?
No
No Further Action
Yes
Isolate any PC/Equipment as potential evidence if appropriate and carry out Investigation
Is Illegal Material or Activity Confirmed?
No
No
Review Incident, Agree and Implement Appropriate Actions
Possible Actions: Inform Parents/Carers Risk Assessment Counselling Referral to Other Agency Community Resolution Disciplinary Procedures
Yes
Allow Police or relevant Organisation to complete their investigations, seeking LADO advice on treatment of Victim / Instigator and possible referral to ISA
Debrief all Relevant Parties at End of e-Safety Incident
Review Policies and Procedures
Police or relevant Organisation take action
Organise Knowledge Share Session

Appendix 1

Acceptable Use of Computing/ICT - Agreement for Children – Early Years & KS1

Computing/Information Communication Technology (ICT) including the internet, email and mobile technology has become an important part of learning in every school. At Ickworth Park we use a filtered internet and secure school email system but we expect all children to be safe and responsible users. Teachers explain the rules below to their class but please also read and discuss these with your child and return the slip at the bottom of this page. Children use Computing/ICT to varying degrees as they progress through the school, according to their age group and the objectives in the National Curriculum. This agreement covers use through your child's time in school and may be updated as technology develops and changes.

My online safety agreement

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

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

Acceptable Use Agreement for Children – reply slip

We have discussed this agreement and…………………………………….......(name) in Class ……………agrees to follow these rules and support the safe use of Computing at Ickworth Park Primary School.

Parent/Carer signature ……..………………….……………………………….

Date ……………………………

Appendix 2

Acceptable Use of Computing/ICT - Agreement for Children – Key Stage 2

Computing/Information Communication Technology (ICT) including the internet, email and mobile technology has become an important part of learning in every school. At Ickworth Park we use a filtered internet and secure school email system but we expect all children to be safe and responsible users. Teachers explain the rules below to their class but please also read and discuss these with your child and return the slip at the bottom of this page. Children use Computing/ICT to varying degrees as they progress through the school, according to their age group and the objectives in the National Curriculum. This agreement covers use through your child's time in school and may be updated as technology develops and changes.

My online safety agreement

- I will look after myself and others by using the internet in a safe and responsible way and only use school ICT for school purposes
- I will only open my own school files
- I will not bring any memory sticks or other storage devices into school
- I will only use the internet with adult permission and only for school learning
- I will only email, open email attachments, chat or message people that a trusted adult has approved as part of my lesson
- I will only send messages that are polite and friendly
- I agree never to fill out forms or give out passwords or personal information like my full name, address or phone numbers
- I agree never to post photographs or video clips without permission and I will not include my name with any photographs
- If I need help I know who I can ask and that I can go to www.thinkuknow.co.uk for help if I cannot talk to an adult
- I know what to do if I see anything on the internet that makes me feel uncomfortable and I will tell an adult immediately
- I will not use or download apps without permission
- I understand that the school may check my computer files and may monitor any internet sites I visit
- I know I should follow these guidelines as part of the agreement with my parent/carer
- I know that if I break these rules I may not be allowed to use school computing equipment

Acceptable Use Agreement for Children – reply slip

We have discussed this agreement and …………………………………….......(name) in Class ……………agrees to follow these rules and support the safe use of Computing at Ickworth Park Primary School.

Parent/Carer signature …….…………………..…………………………….

Date ……………………………

Appendix 3

Acceptable Use of ICT Agreement for Staff, Governors, Volunteers and Visitors

This agreement applies to all online use, mobile communications and anything downloaded or printed. The online safety policy is available in school to refer to about all issues and procedures.
All adults within the school must be aware of their safeguarding responsibilities when using technologies and they are asked to sign this agreement. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- In case of a data breach or personal data I will report this to the Data Protection Officer and Headteacher within the required 72 hours.
- I know that I must only use the school equipment in an appropriate manner and professional manner
- I understand that I need to give permission to children before they can upload images (video or photographs) to the internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of children if uploading to the internet.
- I will report accidental misuse.
- I will report any incidents of concern for a child's safety to the Designated Safeguarding Lead in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Designated Safeguarding Lead is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children via personal technologies, including my personal e-mail. I know I should use the school e-mail address and phones for educational purposes.
- I should complete virus checks on my laptop, memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the current Data Protection legislation and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the Online Safety Lead prior to sharing this information.
- I will adhere to copyright and intellectual property rights and I will only install hardware and software I have been given permission for.
- I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- I will follow the schools guidance on the use of personal mobile phones and other devices.
- I will not use social networking sites to discuss school related issues.

I have read and understood the online safety policy and the Acceptable Use Agreement and know that by following them I have a better understanding of online safety and my responsibilities to safeguard children when using online and mobile technologies.

Signed…………………………………………………. Date…………………….

Name (printed)……………………………………… Role.......................................

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

Online safety training needs audit	
Name of staff member/volunteer:	
Date:	
Do you know the name of the person who has lead responsibility for online safety in school?	
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 IT systems?	
Are you familiar with the school’s approach to tackling cyber-bullying and the school’s Anti-Bullying Policy?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	