**Edward Jenner School**

**Online Safety Policy**

|  |  |  |
| --- | --- | --- |
|  | Date | Signed |
| Reviewed | Sept 2025 | R Dalton/P Brookes |
| Ratified by Head | Sept 2025 | A Brookes |
| Date of next review | September 2026 |  |

# Table of Contents

[Table of Contents 1](#_Toc210724533)

[Development/Monitoring/Review of this Policy 2](#_Toc210724534)

[Additional Documents Relating to Online Safety 4](#_Toc210724535)

[Roles and Responsibilities 5](#_Toc210724536)

[Policy Statements 8](#_Toc210724537)

[Mobile Technologies (including BYOD/BYOT) 12](#_Toc210724538)

[Use of digital and video images 14](#_Toc210724539)

[Data Protection 16](#_Toc210724540)

[Communications 18](#_Toc210724541)

[Home/Remote Learning And Lockdown Response 20](#_Toc210724542)

[Social Media - Protecting Professional Identity 22](#_Toc210724543)

[Dealing with unsuitable/inappropriate activities 24](#_Toc210724544)

[Responding to Online Safety Incidents 26](#_Toc210724545)

[Appendix A – Acceptable Use Policies 31](#_Toc210724546)

[Appendix B - Responding to incidents of misuse – flow charts 48](#_Toc210724551)

[Appendix C – Recording/Reporting Incidents of Misuse 50](#_Toc210724552)

[Appendix D – Relevant Legislation & Guidance 53](#_Toc210724553)

[Appendix E – Key Organisations & Resources 55](#_Toc210724554)

# Development/Monitoring/Review of this Policy

4

This online safety policy has been developed by a Senior Leadership group and staff group made up of:

* Online Safety Officer/Coordinator Phil Brookes
* Designated Safeguard Lead Leigh Allen
* Head Manda Brookes
* Members of staff

|  |  |
| --- | --- |
| The implementation of this online safety policy will be monitored by the: | Senior Leadership Team  Online Safety Coordinator  Online Safety Group  Advisory Board |
| Monitoring will take place at regular intervals: | At least twice a year – unless review of new developments, threats, activities or incidents indicate more frequently |
| The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be: | September 2026 |
| Should serious online safety incidents take place, the following external persons/agencies should be informed: | Safeguarding Children Manager (education) - Georgina Summers ([gsep@gloucestershire.gov.uk](mailto:gsep@gloucestershire.gov.uk) 01452 426221.  LADO – Nigel Hatten ([amadmin@gloucestershire.gov.uk](mailto:amadmin@gloucestershire.gov.uk) 01452 426320)  Police |

The school will monitor the impact of the policy using:

* Logs of reported incidents
* Monitoring logs of internet activity (including sites visited)/filtering records
* Internal monitoring data for network activity
* Surveys/questionnaires of pupils, parents/carers, staff

6

**Scope of the Policy**

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

The Education and Inspections Act 2006 empower Headteachers/Principals to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

# Additional Documents Relating to Online Safety

This Document should be read in conjunction with the following documents:

* EJS Electronic Devices - Pupil Search and Deletion Policy
* EJS Social Media Policy
* EJS Online Safety Group Terms of Reference
* EJS School Technical Security Policy (including filtering and passwords)
* EJS School Personal Data Advice and Guidance
* EJS Acceptable Use Agreement – Pupil, Parent and Staff
* EJS Online Safety Curriculum Plan

# Roles and Responsibilities

7

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

## Headteacher/Principal and Senior Leaders

* The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Lead.
* The Headteacher and (at least) another member of the Senior Leadership Team 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. (see flow chart on Responding to Online Safety Incidents – included in a later section and [Gloucestershire Safeguarding Children Partnership (GSCP)](https://www.gloucestershire.gov.uk/gscp/)
* The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant
* The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles.
* The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead during staff meetings.
* This policy and proposed changes will be reviewed by the Advisory Board at termly meetings and adhoc as required.

## Online Safety Lead

* leads the Online Safety Group
* takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
* ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
* provides training and advice for staff
* liaises with the Local Authority/MAT/relevant body
* liaises with school technical staff
* receives reports of online safety incidents and creates a log of incidents to inform future online safety developments, (see Appendix B)
* meets regularly with SLT and Staff to discuss current issues, review incident logs and filtering/change control logs
* attends relevant meetings of staff meetings
* reports regularly to Senior Leadership Team

## Network Manager/Technical staff

Those with technical responsibilities are responsible for ensuring:

* that the school’s technical infrastructure is secure and is not open to misuse or malicious attack
* that the school meets required online safety technical requirements and any ISA online safety policy/guidance that may apply.
* that users may only access the networks and devices through a properly enforced password protection policy (see policy - EJS School Personal Data Advice and Guidance)
* the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see policy - Technical Security Policy )
  + - that 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
    - that the use of the internet is regularly monitored in order that any misuse/attempted misuse can be reported to theHeadteacherand Online Safety Leadfor investigation/action/sanction

that monitoring software/systems are implemented and updated as agreed in school policies

## Teaching and Support Staff

Are responsible for ensuring that:

* they have an up-to-date awareness of online safety matters and of the current school online safety policy and practices
* they have read, understood and signed the staff acceptable use agreement (AUA)
* they report any suspected misuse or problem to the Online Safety Leadfor investigation/action/sanction
* all digital communications with pupils/parents/carers 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 understand and follow the Online Safety Policy and acceptable use policies
* pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* 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 should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

## Designated Safeguarding Lead

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

* sharing of personal data
* access to illegal/inappropriate materials
* inappropriate on-line contact with adults/strangers
* potential or actual incidents of grooming
* online-bullying

## Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. Depending on the size or structure of the school, this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the Head Teacher.

Members of the Online Safety Group will assist the Online Safety Lead (or other relevant person, as above) with:

* the production/review/monitoring of the school online safety policy/documents.
* the production/review/monitoring of the school filtering policy and requests for filtering changes.
* mapping andreviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
* monitoring network/internet/filtering/incident logs
* consulting stakeholders – including parents/carers and the pupils about the online safety provision
* monitoring improvement actions identified through use of the 360 degree safe self-review tool

## Pupils:

* are responsible for using the school digital technology systems in accordance with the student/pupil acceptable use agreement
* have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
* will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online bullying.
* should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *school’s/academy’s* online safety policy covers their actions out of school, if related to their membership of the school

## Parents/carers

Parents/carers 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’ evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature.* Parents and carers 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
* access to parents’ sections of the website/Learning Platform and on-line student/pupil records
* their children’s personal devices in the school (where this is allowed)

# Policy Statements

## Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *pupils* to take a responsible approach. The education of *pupils* in online safety/digital literacy is therefore an essential part of the school’s online safety provision. Children and young people need the help and support of staff, parents and secure IT systems to learn a positive attitude towards the use of the internet.

Online safety should be a focus in all areas of the curriculum 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 should be provided as part of Computing/PHSE/other lessons and should be regularly revisited
* Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
* Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
* Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
* Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making (additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.)
* Pupils should be helped to understand the need for the pupil acceptable use agreement 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, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
* Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
* It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
* Pupils are reminded at each login with an onscreen desktop to be aware of internet safety:

Text

Description automatically generated with medium confidence

## Education – Pupils with Additional Needs

## The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the school’s Online rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online issues.

## Where a pupil has poor social understanding, careful consideration is to be given to group interactions when raising awareness of Online safety.

Internet activities are to be planned and well managed for additional needs children and young people.

## Education – Parents/carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children’s online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

* Curriculum activities
* Letters, newsletters, the school web site,
* Parents/carers evenings/sessions
* High profile events/campaigns e.g. Safer Internet Day
* Reference to the relevant web sites/publications:
  + www.[swgfl.org.uk](http://swgfl.org.uk),
  + [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/),
  + <http://www.childnet.com/parents-and-carers>

(see appendix for further links/resources)

## Education & Training – Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

* A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
* All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
* The Online Safety Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
* This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
* The Online Safety Lead will provide advice/guidance/training to individuals as required.

Technical – infrastructure, equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities (A more detailed Technical Security Template Policy can be found in the appendix).

* School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
* There will be regular reviews and audits of the safety and security of school technical systems
* Servers, wireless systems and cabling must be securely located and physical access restricted
* All users will have clearly defined access rights to school technical systems and devices.
* All users will be provided with a username and secure password by the IT Manager who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password (good password practice is discussed in appendix)
* The “administrator” passwords for the school systems, used by the IT Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe)
* The IT Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
* **Internet access is filtered for all EJS users.** Illegal content (child sexual abuse images) is filtered by our broadband provider, our requirements for filtering of adult content and PREVENT duty is provided by SECURLY and DNS lookup is via OpenDNS. Content lists are regularly updated, and internet use is logged and regularly monitored
* A request for filtering changes would need to be logged with School Technical Staff and this would be passed to the Online Safety Group for discussion.
* The school has provided enhanced/differentiated user-level filtering
* School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
* Users able to report any actual/potential technical incident/security breach to the school or relevant online authorities using the links in the Bookmark Bar in their browser or via the school website.
* School systems are based on the Chrome browser and use Google Cloud facilities registered to a secure domain, so data is held securely ‘in the cloud’. Equally our ISP provides firewall facilities which protect our routers, and wireless systems. There are no live workstations onsite overnight and during the day these devices are protected by up-to-date virus software and individual firewall settings.
* Guest access of is not provided on site.
* An agreed policy (Pupil and Parent AUA) is in place regarding the extent of personal use that users and their family members are allowed on school devices that may be used out of school.
* An agreed policy (Staff AUA) is in place that forbids staff from downloading executable files and installing programmes on school devices.
* An agreed policy (EJS School Personal Data Advice and Guidance) is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured*.* (See EJS School Personal Data Advice and Guidance for further detail)

# Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilizing the school’s wireless network. The device then has access to the wider internet which may include the school’s learning platform and other cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The school’s stance on mobile technologies can be found in the EJS Electronic Devices and Pupil Search and Deletion Policy and references safeguarding policy, behaviour policy, bullying policy and procedures around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school’s online safety education Plan.

The school Acceptable Use Agreements for staff, pupils and parents/carers considers the use of mobile technologies. See Appendix A for agreement and risk assessment for personal devices

The school allows:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | School Devices | | | Personal Devices | | |
|  | **School owned for single user** | **School owned for multiple users** | **Authorised device[[1]](#footnote-1)** | **Student owned** | **Staff owned** | **Visitor owned** |
| Allowed in school | Yes | Yes | Yes | Yes – for Y10+ | Yes | Yes |
| Full network access | Yes | Yes | Yes | No | No | No |
| Internet only | Yes | Yes | Yes | No | Yes | No |
| No network access | Yes | Yes | Yes | No | No | No |

At time of writing the following aspects will be considered by the Online Safety Group and be included in an update to the Online Safety Policy:

## For School owned/provided devices:

* *Who they will be allocated to*
* *Where, when and how their use is allowed – times/places/in school/out of school*
* *If personal use is allowed*
* *Levels of access to networks/internet (as above)*
* *Management of devices/installation of apps/changing of settings/monitoring*
* *Network/broadband capacity*
* *Technical support*
* *Filtering of devices*
* *Access to cloud services*
* *Data Protection*
* *Taking/storage/use of images*
* *Exit processes – what happens to devices/software/apps/stored data if user leaves the school*
* *Liability for damage*
* *Staff training*

## For Personal devices:

* Which users are allowed to use personal mobile devices in school (staff/pupils/students/visitors)
* Restrictions on where, when and how they may be used in school
* Storage
* Whether staff will be allowed to use personal devices for school business
* Levels of access to networks/internet (as above)
* Network/broadband capacity
* Technical support (this may be a clear statement that no technical support is available)
* Filtering of the internet connection to these devices
* Data Protection
* The right to take, examine and search users’ devices in the case of misuse (England only) – N.B. this must also be included in the Behaviour Policy.
* Taking/storage/use of images
* Liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility).
* Identification/labelling of personal devices
* How visitors will be informed about school requirements
* How education about the safe and responsible use of mobile devices is included in the school online safety education programmes.

# Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks to reduce the likelihood of the potential for harm:

* When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
* Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press
* In accordance with guidance from the Information Commissioner’s Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images. Warnings are issued at all events involving parents/carers.
* Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
* Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
* Pupils must not take, use, share, publish or distribute images of others without their permission.
* Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images (see EJS School Personal Data Advice and Guidance and EJS Electronic Devices and Pupil Search and Deletion Policy for further details).
* Pupil’s full names will not be used anywhere on a website or blog, particularly in association with photographs.
* Pupil’s work can only be published with the permission of the pupil and parents or carers.

**Safe Use of AI**

The OSG continually reviews the developmnet of AI and sets out expectations for the safe, ethical, and responsible use of Artificial Intelligence (AI) tools by pupils in school. It supports digital literacy, safeguarding, and academic integrity.

**Scope**

* Applies to all pupils at EJS
* Covers use of AI on school devices, personal devices when on site, and when revising / studying at home.

**1. Responsible Use**

* AI may be used for learning support (e.g. generating ideas, checking grammar, practising questions) when authorised by a teacher.
* Pupils must not use AI to replace original work in assessments, homework, or coursework. Plagiarism rules apply.
* Pupils should always credit AI tools when used for research or inspiration.

**2. Safety and Safeguarding**

* Pupils must not use AI to generate, share, or request harmful, offensive, or inappropriate content.
* AI should never be used to impersonate, bully, or harass others.
* Any concerning content produced by AI must be reported to a teacher immediately.

**3. Data and Privacy**

* Personal information (e.g. names, photos, contact details) must never be entered into AI systems.
* Pupils should only use school-approved AI tools to ensure compliance with data protection (GDPR).

**4. Academic Integrity**

* AI outputs are to be used as supporting tools, not final submissions.
* Pupils remain responsible for the accuracy, originality, and quality of their work.
* Teachers may require pupils to explain or show evidence of their own understanding.

**5. Monitoring and Consequences**

* Staff may review use of AI in line with this ICT Acceptable Use Policy.
* Misuse of AI (e.g. plagiarism, harmful content, data breaches) will result in disciplinary action under the behaviour policy.

# Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

## The school seeks to ensure that:

* it has a Data Protection Policy. (EJS School and Personal Data Advice and Guidance
* it implements the data protection principles and can demonstrate that it does so through use of policies, notices and records.
* it has paid the appropriate fee Information Commissioner’s Office (ICO) and included details of the Data Protection Officer (DPO).
* it has appointed a Data Protection Officer (DPO)
* it has an ‘Information Asset Register’ in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
* the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
* it will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a ‘retention policy” to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
* it provides staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the EJS School and Personal Data Advice and Guidance document)
* procedures are in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them (subject to certain exceptions which may apply).
* Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
* IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners.
* it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
* it understands how to share data lawfully and safely with other relevant data controllers.
* it [reports any relevant breaches to the Information Commissioner](https://ico.org.uk/for-organisations/report-a-breach/) within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. To do this, EJS has a set up the Online Safety Group for reporting, logging, managing, investigating and learning from information risk incidents.
* all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking data protection functions, such as handling requests under the individual’s rights, will receive training appropriate for their function as well as the core training provided to all staff.

## When personal data is stored on any mobile device or removable media staff know that:

* Data must be encrypted and password protected.
* The device must be password protected.
* The device must be protected by up-to-date virus and malware checking software

16

* Data must be securely deleted from the device, in line with school policy (see - EJS School and Personal Data Advice and Guidance) once it has been transferred or its use is complete.

## Staff must ensure that they:

* at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
* can recognise a possible breach, understand the need for urgency and know who to report it to within the school
* can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
* where personal data is stored or transferred on mobile or other devices (including USB Drives) these must be encrypted and password protected.
* will not transfer any school personal data to personal devices except as in line with school policy
* access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly “logged off” at the end of any session in which they are using personal data
* Transfer pupil data only when necessary and only within the school. All external requests for data must go via the Head Teacher or the Data Protection Manager.
* The EJS School and Personal Data Advice and Guidance provides more detailed information on the school’s responsibilities and on good practice.

# Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Staff & other adults | | | Pupils | | | |
| Communication Technologies | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed below KS4 | Allowed at certain times | Allowed with staff permission | Allowed for certain Year groups | |
| Mobile phones may be brought to the school | ✓ |  |  | ✓ | ✓ | 🗶 | ✓ | |
| Use of mobile phones in lessons | 🗶 | 🗶 | ✓ | 🗶 | 🗶 | 🗶 | 🗶 | |
| Use of mobile phones in social time | ✓ | ✓ |  | ✓ | 🗶 | 🗶 | ✓ | |
| Taking photos on School mobile phones/cameras | ✓ | ✓ | ✓ | 🗶 | ✓ | ✓ | ✓ | |
| Use of other mobile devices e.g. tablets, gaming devices | ✓ | ✓ | 🗶 | 🗶 | ✓ | ✓ | ✓ | |
| Use of personal email addresses in school, or on school network | 🗶 | ✓ | ✓ | 🗶 | 🗶 | 🗶 | 🗶 | |
| Use of school email for personal emails | 🗶 | 🗶 | 🗶 | 🗶 | 🗶 | 🗶 | 🗶 | |
| Use of messaging apps | 🗶 | ✓ | 🗶 | 🗶 | ✓ | 🗶 | ✓ | |
| Use of social media | 🗶 | ✓ | ✓ | 🗶 |  | 🗶 | ✓ | |
| Use of blogs | 🗶 | 🗶 | 🗶 | 🗶 | 🗶 | 🗶 | 🗶 | |

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

* The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
* Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication**.**
* Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, VLE etc) 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.
* Whole class/group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.
* Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be 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.

# Home/Remote Learning And Lockdown Response

In the event of a Lockdown order EJS staff continue to do what they reasonably can to keep all children safe. During the time of the emergency most children enrolled at EJS will not be physically attending the school. It is therefore important that all staff who interact with children online continue to look out for signs a child may be at risk. Any concerns should be reported to the DSL or DDSL by telephone and a written report should be emailed at the earliest opportunity. Safeguarding procedures outlined in the EJS Safeguarding Policy will be implemented.

At EJS we have a culture of educating the children and parents regularly about online safety. This role falls to all staff. The children know what to do if they are faced with harmful content or where to go if they need help and support online (see Appendix E- Links to other organisations or documents). The EJS Acceptable User Agreement issued to all staff and children applies. We ensure that appropriate filtering and monitoring systems are in place. Recommended learning websites are checked by our IT manager if they are not normally utilised in the classroom. In the case of our IT manager not being available the role will move remotely to Mr G Rees IT and Cyber Consultant. At EJS we ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

At EJS we are in regular contact with parents and carers. We use these communications to reinforce the importance of children being safe online. Parents and carers are made aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school their child is going to be interacting with online. Parents have information websites signposted for them (see Appendix E- Links to other organisations or documents) to ensure they have all the information they need to keep their children safe online. We encourage the parents to seek further information from school if they are worried. Parents are encouraged to work alongside their child if it is possible.

EJS has adopted an a 2-tier active approach to remote learning. Via Edward Jenner School’s Google Education Account and within that using Google Classroom Meets staff will provide a regular series of curriculum focused online meetings. Pupils are invited via secure email to attend directed meetings with staff and other pupils. Additionally, and for those pupils unable to join via the internet, work is posted by staff via mail directly to individual pupils. This can include specific documents, document links to our Google Classroom drive areas or links to existing public websites. Pupils download their individual work, complete it and email/send it directly back to their teacher. The learning interaction is solely with their existing teacher with possibly interaction with parents as guides. It is not expected that this will become a long-term or permanent feature of teaching and learning at EJS. Staff are not expected to interact in real-time with any individual or group of pupils via anything other than the EJS Google Classroom system as described here. These emails are monitored by EJS.

**Remote Learning and Safeguarding**

Any interaction with pupils is governed by the rules set out in the **EJS Staff Code of Conduct**. This includes the acceptable use of technologies, staff–student relationships, and communication (including the use of social media).

Further guidance on safe remote learning is available from the **UK Safer Internet Centre** and through the Department for Education (DfE):

* [Safeguarding and remote education](https://www.gov.uk/guidance/safeguarding-and-remote-education) (DfE)
* [Coronavirus (COVID-19): safeguarding in schools, colleges and other providers](https://www.gov.uk/government/publications/covid-19-safeguarding-in-schools-colleges-and-other-providers/coronavirus-covid-19-safeguarding-in-schools-colleges-and-other-providers) (DfE)

Parents and carers may choose to supplement the school’s online offer with support from external organisations or individual tutors. In our communications with parents and carers, we emphasise the importance of securing online support from a **reputable organisation or individual** who can provide evidence of safe practice, safeguarding checks, and suitability to work with children.

# Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools are responsible, indirectly, for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm from online sources to pupils, staff and the school through:

* Ensuring that personal information is not published
* Training is provided including:
  + acceptable use.
  + social media risks.
  + checking of settings.
  + data protection.
  + reporting issues.
* Clear reporting guidance, including responsibilities, procedures and sanctions
* Risk assessment, including legal risk

School staff should ensure that:

* No reference should be made in social media to pupils, parents/carers or school staff
* They do not engage in online discussion on personal matters relating to members of the school community
* Personal opinions should not be attributed to the school or local authority
* Security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information

## Official school social media accounts should maintain:

* A process for approval by senior leaders
* Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
* A code of behaviour for users of the accounts, including:
  + Systems for reporting and dealing with abuse and misuse
  + Understanding of how incidents may be dealt with under school disciplinary procedures

## Personal Use

* Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
* Personal communications which do not refer to or impact upon the school are outside the scope of this policy
* Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

## Monitoring of Public Social Media:

* The school has developed the EJS Social Media Policy
* As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
* The school should effectively respond to social media comments made by others according to a defined policy (EJS Social Media Policy)

The school’s use of social media for professional purposes will be checked regularly by the Online Safety Group to ensure compliance with the school policies.

# Dealing with unsuitable/inappropriate activities

Some internet activities e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| User Actions  18 | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
| Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978  N.B. Schools/academies should refer to guidance about dealing with self-generated images/sexting – [UKSIC Responding to and managing sexting incidents](https://swgfl.org.uk/assets/documents/managing-sexting-incidents.pdf?_=1554476329) and [UKCIS – Sexting in schools and colleges](https://www.gov.uk/government/publications/sexting-in-schools-and-colleges) |  |  |  |  | X |
| Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003. |  |  |  |  | X |
| Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008 |  |  |  |  | X |
| 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 |  |  |  |  | X |
| Pornography |  |  |  | X |  |
| Promotion of any kind of discrimination |  |  |  | X |  |
| threatening behaviour, including promotion of physical violence or mental harm |  |  |  | X |  |
| Promotion of extremism or terrorism |  |  |  | X |  |
| Peer on Peer abuse - any kind of sexual, emotional or financial abuse or coercive control exercised between children online |  |  |  | X |  |
| Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute |  |  |  | X |  |
| Activities that might be classed as cyber-crime under the Computer Misuse Act:   * Gaining unauthorised access to school networks, data and files, through the use of computers/devices * Creating or propagating computer viruses or other harmful files * Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) * Disable/Impair/Disrupt network functionality through the use of computers/devices * Using penetration testing equipment (without relevant permission)   The school will decide on an incident-by-incident basis if the matter is to be delt with internally or by the Police | |  |  |  |  | X |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school | |  |  |  | X |  |
| Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords) | |  |  |  | X |  |
| Unfair usage (downloading/uploading large files that hinders others in their use of the internet) | |  |  |  | X |  |
| Using school systems to run a private business | |  |  |  | X |  |
| Infringing copyright | |  |  |  | X |  |
| On-line gaming (educational) | |  | ✓ | ✓ |  |  |
| On-line gaming (non-educational) | |  |  | ✓ | 🗶 |  |
| On-line gambling | |  |  |  | 🗶 |  |
| On-line shopping/commerce | |  |  | ✓ |  |  |
| File sharing | |  |  | ✓ |  |  |
| Use of social media | |  |  | ✓ |  |  |
| Use of messaging apps | |  | ✓ |  |  |  |
| Use of video broadcasting e.g. YouTube  19 | |  |  | ✓ |  |  |

# Responding to Online Safety Incidents

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

## Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.

Diagram

Description automatically generated

## 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.

In the event of suspicion, all steps in this procedure should be followed:

* Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
* Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
* 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).
* Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. 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 form (except in the case of images of child sexual abuse – see below)
* Once this has been completed and fully investigated the group will need to 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
  + Involvement by Local Authority or national/local organisation (as relevant).
  + Police involvement and/or action
* **If content being reviewed includes images of child abuse, then the monitoring should be halted and 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
  + adult material which potentially breaches the Obscene Publications Act
  + criminally racist material
  + promotion of terrorism or extremism
  + offences under the Computer Misuse Act (see User Actions chart above)
  + other criminal conduct, activity or materials
* **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all 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 form should be retained by the group for evidence and reference purposes.

## School actions & 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, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

|  |
| --- |
|  |
| Pupils Incidents | Refer to class teacher | | | Refer to Headteacher/Head of School | | Refer to Police | | Refer to technical support staff for action re filtering/security etc. | | Inform parents/carers | | Removal of network/internet access rights | | Warning | | Further sanction e.g. detention/exclusion |
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).** |  | | | X | | X | | X | | X | | X | |  | | X |
| Unauthorised use of non-educational sites during lessons | X | | | X | |  | | X | | X | | X | | X | | X |
| Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device | X | | | X | |  | |  | | X | |  | | X | | X |
| Unauthorised/inappropriate use of social media/ messaging apps/personal email |  | | | X | |  | | X | | X | | X | | X | | X |
| Unauthorised downloading or uploading of files |  | | | X | |  | | X | | X | | X | | X | | X |
| Allowing others to access school network by sharing username and passwords | X | | |  | |  | | X | |  | | X | | X | |  |
| Attempting to access or accessing the school network, using another student’s/pupil’s account | X | | |  | |  | | X | |  | | X | | X | | X |
| Attempting to access or accessing the school network, using the account of a member of staff |  | | | X | |  | | X | | X | | X | | X | | X |
| Corrupting or destroying the data of other users |  | | | X | |  | | X | | X | | X | |  | | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | | | X | |  | | X | | X | | X | | X | | X |
| Continued infringements of the above, following previous warnings or sanctions |  | | | X | | X | | X | | X | | X | |  | | X |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school |  | | | X | |  | | X | | X | | X | |  | | X |
| Using proxy sites or other means to subvert the school’s filtering system |  | | | X | |  | | X | | X | | X | |  | | X |
| Accidentally accessing offensive or pornographic material and failing to report the incident | X | | | X | |  | | X | |  | | X | | X | | X |
| Deliberately accessing or trying to access offensive or pornographic material | X | | | X | |  | | X | | X | | X | | X | | X |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act  21 |  | | | X | |  | | X | | X | | X | | X | | X |
|  | | | |
| Staff Incidents | | | Refer to Local Authority/HR | | | Refer to Police | | Refer to Technical Support Staff for action re filtering etc. | | Warning | | Suspension | | Disciplinary action | |
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).** | | | X | | | X | | X | | X | | X | | X | |
| Inappropriate personal use of the internet/social media/personal email | | |  | | |  | | X | | X | |  | | X | |
| Unauthorised downloading or uploading of files | | |  | | |  | | X | | X | |  | | X | |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person’s account | | |  | | |  | | X | | X | |  | |  | |
| Careless use of personal data e.g. holding or transferring data in an insecure manner | | |  | | |  | | X | | X | | X | | X | |
| Deliberate actions to breach data protection or network security rules | | |  | | |  | | X | | X | | X | | X | |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | | |  | | |  | | X | | X | |  | | X | |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | | |  | | |  | |  | | X | |  | | X | |
| Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with pupils | | | X | | | X | |  | | X | | X | | X | |
| Actions which could compromise the staff member’s professional standing | | | X | | |  | |  | | X | | X | | X | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | | |  | | |  | | X | | X | |  | | X | |
| Using proxy sites or other means to subvert the school’s/academy’s filtering system | | |  | | |  | |  | | X | |  | | X | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | | |  | | |  | | X | | X | |  | | X | |
| Deliberately accessing or trying to access offensive or pornographic material | | |  | | |  | | X | | X | | X | | X | |
| Breaching copyright or licensing regulations | | |  | | |  | | X | | X | |  | | X | |
| Continued infringements of the above, following previous warnings or sanctions | | |  | | |  | |  | |  | | X | | X | |

22

See Appendix B - Responding to incidents of misuse – flow charts

# Appendix A – Acceptable Use Policies

# Edward Jenner School Pupil Acceptable Use Agreement (2025)

## School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

## This acceptable use agreement is intended to ensure:

* that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
* that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users.

## Acceptable Use Agreement:

**For my own personal safety:**

* I understand that the school will monitor my use of the systems, devices and digital communications.
* I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person’s username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
* I will be aware of “stranger danger”, when I am communicating on-line.
* I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
* If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
* I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
* I will keep my username and password a secret, I will not share them with anyone. Choose a **strong password** you can remember without writing it down. If you think someone knows your password, tell a teacher immediately.
* I will tell my teacher if I receive an email or message from someone I do not recognise. Be cautious of messages that ask you for personal information, tell you to download something, or promise something that sounds too good to be true. **Never click on a link or open an attachment from an unknown sender.**
* I will not share personal information such as my full name, address, phone number, school name, or photos without a parent's or teacher's permission. Be careful about what you post, as it can be difficult to remove once it's online.

**I understand that everyone has equal rights to use technology as a resource and:**

* I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use.
* I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
* I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube).

25

**I will act as I expect others to act toward me:**

* I will respect others’ work and property and will not access, copy, remove or otherwise alter any other user’s files, without the owner’s knowledge and permission.
* I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
* I will not take or distribute images of anyone without their permission.

**I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:**

* I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have direct permission from the Headteacher. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
* I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
* I will immediately report any damage or faults involving equipment or software, however this may have happened.
* I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
* I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
* I will not use social media sites during school time on school devices.

**When using the internet for research I recognise that:**

* I should ensure that I have permission to use the original work of others in my own work
* Where work is protected by copyright, I will not try to download copies (including music and videos)
* When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

**I am responsible for my actions, both in and out of school:**

* I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online bullying, use of images or personal information).
* I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

The following activities are strictly prohibited when using school technology:

**Please complete the section on the next page to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices – this will have a detrimental effect on your learning.**

# Edward Jenner School Pupil Acceptable Use Agreement (2025)

## Sign and Return

This form relates to the *student/pupil* acceptable use agreement; to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. When signed please return this sheet to your teacher, you must keep the other 2 attached sheets.

If you do not sign and return this agreement, access will not be granted to school systems and devices – this will have a detrimental effect on your learning

I have read and understood the above. I agree and understand that:

* I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.
* I use the school systems and devices (both in and out of school) for educational purposes only.
* I should not use my own devices in school (e.g. mobile phones, USB devices, cameras etc.) unless explicitly told otherwise.
* If I use my own equipment out of school in a way that is related to me being a member of this school (e.g. communicating with other members of the school, accessing school email, learning platform, website etc.) I must abide by the above AUA.

Name of Student/Pupil:

Signed:

Date:

# Acceptable Use Policy (AUP) – Pupil Mobile Phone Use

## Purpose

This policy sets out clear expectations for the responsible use of personal mobile phones by pupils in school, ensuring learning, safety, and wellbeing are prioritised.

• Applies to all pupils on school premises, school trips, and any school-related activities.  
• Covers smartphones, smartwatches, tablets with SIM capability, and similar devices.

## 1. General Rules

• Phones must be switched off or set to silent and kept out of sight during lessons, unless a teacher permits their use for learning purposes.  
• Phones may be used at break and lunch times only in designated areas by Y11 *[all others at the discretion of individual risk assessment]* (Y11 Bat / Century House).  
• Pupils must not use phones to make or receive calls, send texts, or access social media during learning time.  
• Phones may be confiscated if used inappropriately, in line with the school’s behaviour policy.

## 2. Safeguarding and Safety

• Pupils must never use phones to bully, harass, or intimidate others (including via social media or messaging apps).  
• Use of phones for taking photos, videos, or audio recordings on school premises is prohibited.  
• Pupils must not share or access inappropriate or illegal content. This includes explicit material, violent images, or extremist content.

## 3. Learning Use

• Teachers do not instruct or expect pupils to use their personal devices for school learning purposes. There are educational devices for this purpose.   
• Misuse during learning tasks may result in withdrawal of permission.

## 4. Security & Responsibility

• Pupils bring phones at their own risk. The school does not accept liability for loss, theft, or damage.  
• Phones should be password/PIN protected.  
• Sharing devices, accounts, or passwords is not permitted.

## Acknowledgement

I have read and understood the Acceptable Use Policy for mobile phones. I agree to follow the rules set out above.  
  
Pupil Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_  
  
Parent/Carer Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_

# Individual Risk Assessment – Pupil Mobile Phone Use

Pupil Name:   
Year Group:

Date of Assessment:

Individual needs / circumstances:  
  
*Example:*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk Area** | **Possible Hazard** | **Likelihood** | **Impact** | **Control Measures** |
| Distraction in lessons | Off-task behaviour, reduced learning time | Medium | Medium | Clear rules, teacher monitoring, restricted use |
| Cyberbullying / peer conflict | Negative messages, social media misuse | Medium | High | Safeguarding policy, monitoring, pastoral support |
| Inappropriate content access | Viewing/sharing harmful or explicit material | Low–Medium | High | Filtering on school Wi-Fi, education on safe use |
| Privacy breaches | Photos/videos taken without consent | Medium | High | Ban on unauthorised recording, staff vigilance |
| Loss/theft of phone | Disputes, safeguarding concerns | Medium | Medium | Parental responsibility, lockers, reporting system |
| Contact with strangers | Grooming, online exploitation | Low | High | Online safety education, parental engagement |
| Mental health impact | Overuse, social pressure, anxiety | Medium | High | PSHE curriculum, wellbeing monitoring |

## Control Measures in Place

• Clear AUP signed by pupil and parent  
• Staff enforcement of rules  
• Pastoral and safeguarding support  
• Education on online safety (PSHE/assemblies)  
• Confiscation procedures  
• Parental engagement and communication

## Residual Risk

Overall risk level: Low / Medium / High (assessor to complete)

## Review

Review date:   
Reviewed by:

**🤖 Safe Use of AI – EJS Pupil Guide**

**👍 You Can:**

* Use AI to **help you learn** – ideas, grammar checks, practice questions.
* You must ask a teacher beforehand to check it is safe and appropriate to do so.
* Credit AI tools if they helped you with research or planning.

**🚫 You Must Not:**

* Copy AI work and hand it in as your own.
* Use AI to create or share **rude, harmful, or unsafe content**.
* Enter **personal details** (like your name, photo, address, or passwords).
* Use AI to bully, trick, or pretend to be someone else.

**📚 Remember:**

* AI is a **tool, not a replacement** for your thinking.
* You are responsible for checking the accuracy of AI answers.
* Teachers may ask you to explain your work to prove you understand it.

**⚠️ If Something Goes Wrong:**

* Tell a teacher if AI shows you anything worrying or unsafe.
* Misuse of AI will lead to the same consequences as breaking ICT rules.

⭐ **Use AI wisely – it’s here to support your learning, not to do the learning for you.**

**Parent/Carer Acceptable Use Agreement**

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should always have an entitlement to safe internet access.

**This acceptable use policy is intended to ensure:**

* that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
* that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
* that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the pupil acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school’s work.

**Permission Form**

As the parent/carer of the above pupil(s), I give permission for my son(s)/daughter(s) to have access to the internet and to ICT systems at school.

I know that my son/daughter has signed an acceptable use agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I have read through the acceptable use agreement with my son/daughter.

I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son’s/daughter’s activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child’s online safety.

As the school is collecting personal data by issuing this form, we are informing you that the information gathered will be:

|  |
| --- |
| Held in this print form on file and consent information only transferred to our pupil data file |
| Accessed only by designated staff in the appropriate pursuit of tasks consistent with the continuing education of your child. |
| Stored in this printed form in a locked filing cabinet and held as a data file online in a secure domain-based Google Cloud account |
| Held for a period of no more than 1 year or until the start of the next academic year. |
| The form will be destroyed by cross-cut shredding and deletion of the data file. |

Parent/Carers Name:

Student/Pupil Name:

Signed:

Date:

**Use of Digital/Video Images Permission**

The use of digital/video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and in public media. Where an image is publicly shared by any means, only your child’s first name will be used.

The school will comply with the Data Protection Act and request parent’s/carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner’s Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *pupils* in the digital/video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

As the school is collecting personal data by issuing this form, we are informing you that the information gathered may be:

|  |
| --- |
| Held in digital form, duplicated to our website and social media account |
| Produced and accessed only by designated staff to record evidence of activities in lessons and out of school in the appropriate pursuit of tasks consistent with the continuing education of your child.  Used to share with and inform current parents of the achievements and activities of their child.  Used to promote the positive image of the school in the public domain to ensure the continuation of the school as a viable business. |
| Held as a data file online in a secure domain-based Google Cloud account.  Uploaded to the school Facebook social media page. |
| Held for a period of no more than 3 year after the child has left the school |
| Destroyed by deletion from our cloud storage and where possible a request made to be removed from social media |

**Digital/Video Images Permission Form**

|  |  |
| --- | --- |
| As the parent/carer of the above student/pupil, I agree to the school taking digital/video images of my child/children. | Yes/No |
| I agree to these images being used: |  |
| * to support learning activities. | Yes/No |
| * in publicity that reasonably celebrates success and promotes the work of the school. | Yes/No |
| * in social media posts on Facebook to inform and celebrate pupil activities and achievement | Yes/No |
| I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images. | Yes/No |

Parent/Carers Name:

Student/Pupil Name:

Signed:

Date:

**Use of Cloud Systems Permission Form**

The school uses Google Workspace for Education Fundamentals – a secure, domain-based, cloud hosted, virtual learning environment to provide online accessfor pupils and staff. This permission form describes the tools and pupil responsibilities for using these services.

The following services are available to each pupil as part of the school’s online presence in Google Workspace for Education (GSuite).

Using GSuitewill enable your child to collaboratively create, edit and share files and websites for educated related projects and communicate via email with other pupils and members of staff. These services are entirely online and available 24/7 from any internet-connected computer.

The school believes that use of the tools significantly adds to your child’s educational experience. These tools were of great benefit during the lockdown period.

As the school is collecting personal data and sharing this with a third party, it is the school’s duty to inform parents/carers that some personal pupil data may be:

|  |
| --- |
| Held in digital form and shared with the above service provider (Google). |
| Produced and accessed only by designated staff to provide secure login and access to online services.  Generated as evidence of activities in lessons and out of school, task assessment data or in the appropriate pursuit of tasks consistent with the continuing education of your child.  Used as an access key to other trusted websites and learning tools. |
| Held as a data file online in a secure domain-based Google Cloud account. |
| Held for a period of no more than 3 year after the child has left the school. |
| Destroyed by deletion from our cloud storage domain and a request for cataloguing and deletion may be made to the school. |

|  |  |
| --- | --- |
| Do you consent to your child to having access to this service? | Yes/No |

Student/Pupil Name:

Parent/Carers Name:

Signed:

Date:

## Edward Jenner School Staff (and Volunteer) Acceptable Use Policy Agreement (2025)

### School Policy

New technologies have become integral to the lives of children and young people in today’s society, both within schools/academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

### This acceptable use policy is intended to ensure:

* that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
* that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
* that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

### Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

### For my professional and personal safety:

* I understand that the school will monitor my use of the school digital technology and communications systems.
* I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, GSuite etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
* I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for considered educational and personal access as detailed in the Online Safety Policy.
* I will not disclose my username or password to anyone else, nor will I try to use any other person’s username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
* I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

28

* I am aware of my duty to ensure that the filtering and monitoring systems are in place and effective to protect students and myself from harmful content.

### I will be professional in my communications and actions when using school systems:

* I will not access, copy, remove or otherwise alter any other user’s files, without their express permission.
* I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
* I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school’s policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website or in pupil work) it will not be possible to identify by name, or other personal information, those who are featured.
* I will only use social networking sites in school in accordance with the school’s policies set out in the Online Safety Policy.
* I will only communicate with pupils and parents/carers using official school systems (use of any personal communication avenues will put you at risk). Any such communication will be professional in tone and manner.
* I will not engage in any on-line activity that may compromise my professional responsibilities.

### The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

* When I use my mobile devices in school it will be solely for personal communication. I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
* I will not use personal email addresses on the school ICT systems.
* I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
* I will ensure that my data is regularly backed up to Google Drive in GSuite, in accordance with relevant school policies.
* I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
* I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
* I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this has been sanctioned by the relevant IT technical staff.
* I will not disable or cause any damage to school equipment, or the equipment belonging to others.
* I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
* I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority (if in doubt check and double check).
* I will immediately report any damage or faults involving equipment or software, however this may have happened.

### When using the internet in my professional capacity or for school sanctioned personal use:

* I will ensure that I have permission to use original work of others in my own work
* Where work is protected by copyright, I will not download or distribute copies (including music and videos).
* I am required to complete mandatory cybersecurity awareness training at least annually.
* I will endeavour to use good cyber-security awareness in all my online actions
* I will promptly report any suspected security incidents, weaknesses, or policy violations. This includes, but is not limited to:
  + Lost or stolen devices.
  + Suspicious emails (phishing).
  + Unusual system behaviour or unauthorized access attempts.
  + Data exposure or potential breaches.
* I will use strong, unique passwords for my school accounts. (Passwords must meet the complexity requirements e.g., length, mix of characters).
* I will enable and use MFA (Multi-Factor Authentication) wherever it is available for school accounts.
* I will never share passwords with anyone, including managers or IT staff (Passwords should not be written down or stored in an unsecure location, they should always be stored in the Password Manager in your Google login).
* I will lock my screen or log out of my computer and devices when leaving them unattended, even for a short period.

### Data handling and communicating with external organisations or people:

* I will ensure that I understand and adhere to the school's Data Protection Policy. Data should be handled, stored, and shared according to its sensitivity level.
* I will ensure that confidential documents are not left unattended on desks or near printers. All physical documents containing sensitive information must be stored securely or shredded when no longer needed.
* I will exercise extreme caution when handling emails from unknown senders. I will not open suspicious attachments, click on unknown links, or provide personal or company information in response to unverified requests (this could be termed Phishing and/or Social Engineering). All school related emails including parent correspondence should go through [office@edwardjennerschool.org](mailto:office@edwardjennerschool.org).
* I will not use personal email accounts to send or receive confidential or sensitive school information or data. All school-related communications should be conducted through office@edwardjennerschool.org.
* I will not use school email for sending unsolicited "junk mail" (spam), creating chain letters, or engaging in any form of harassment.
* I will exercise maximum caution when using external storage devices (e.g., USB drives). They must be scanned for malware before being connected to the school network. I will not use personal storage devices to transfer school data unless explicitly authorized.

## Edward Jenner School Staff (and Volunteer) Acceptable Use Policy Agreement (2025)

### I understand that I am responsible for my actions in and out of the school:

* I understand that the attached acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
* I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to directors and/or the Local Authority and in the event of illegal activities the involvement of the Police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name:

Signed:

Date:

# Appendix B - Responding to incidents of misuse – flow charts

Diagram

Description automatically generated

### Diagram Description automatically generated

# Appendix C – Recording/Reporting Incidents of Misuse

**Record of reviewing devices/internet sites (responding to incidents of misuse)**

Group:

Date:

Reason for investigation:

### Details of first reviewing person

Name:

Position:

Signature:

### Details of second reviewing person

Name:

Position:

Signature:

### Name and location of computer used for review (should be discreet machine for web sites)

|  |  |
| --- | --- |
| Web site(s) address/device | Reason for concern |
|  |  |
|  |  |
|  |  |

Conclusion and Action proposed or taken

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

## Reporting Log

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Group: | | | | | | |
| Date | Time | Incident | Action Taken | | Incident Reported By | Signature |
| What? | By Whom? |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

## Training Needs Audit Log

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Group: | | | | |
| Relevant training the last 12 months | Identified Training Need | To be met by | Cost | Review Date |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Appendix D – Relevant Legislation & Guidance

Schools should be aware of the legislative and statutory framework underpinning this online safety policy. In general, an action that is illegal offline is also illegal online. Legal advice should be sought in serious or ambiguous cases.

## Statutory Safeguarding & Education Guidance

Keeping Children Safe in Education (DfE, effective 1 September 2025) — statutory guidance for safeguarding in schools in England. Available at: <https://assets.publishing.service.gov.uk/media/68add931969253904d155860/Keeping_children_safe_in_education_from_1_September_2025.pdf>

Searching, screening and confiscation: Advice for Schools (DfE, July 2022) — current guidance on school powers to search pupils and confiscate items. Available at: <https://www.gov.uk/government/publications/searching-screening-and-confiscation>

## Criminal & Civil Legislation

**Appendix D – Relevant Legislation & Guidance**

The following legislation underpins online safety responsibilities in schools. Each Act is linked to the official source for reference.

|  |  |  |
| --- | --- | --- |
| **Act / Legislation** | **Relevance to Schools** | **Link** |
| Computer Misuse Act 1990 | Offences of unauthorised access, hacking, misuse of computer material | <https://www.legislation.gov.uk/ukpga/1990/18> |
| Data Protection Act 2018 & UK GDPR | Governs processing and protection of personal data | <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted> |
| Freedom of Information Act 2000 | Right of access to information held by public authorities | <https://www.legislation.gov.uk/ukpga/2000/36/contents> |
| Communications Act 2003 | Regulates harmful or offensive electronic communications | <https://www.legislation.gov.uk/ukpga/2003/21/contents> |
| Malicious Communications Act 1988 | Offence to send indecent, offensive or threatening communications | <https://www.legislation.gov.uk/ukpga/1988/27/contents> |
| Regulation of Investigatory Powers Act 2000 | Lawful interception and monitoring of communications | <https://www.legislation.gov.uk/ukpga/2000/23/contents> |
| Investigatory Powers Act 2016 | Updated framework for lawful interception and retention of data | <https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted> |
| Trademarks Act 1994 | Protects registered trademarks from misuse | <https://www.legislation.gov.uk/ukpga/1994/26/contents> |
| Copyright, Designs and Patents Act 1988 | Protects copyright works including digital materials | <https://www.legislation.gov.uk/ukpga/1988/48/contents> |
| Telecommunications Act 1984 | Older offences relating to communications systems | <https://www.legislation.gov.uk/ukpga/1984/12/contents> |
| Criminal Justice & Public Order Act 1994 | Includes harassment and disorder offences | <https://www.legislation.gov.uk/ukpga/1994/33/contents> |
| Racial and Religious Hatred Act 2006 | Criminalises inciting hatred on religious grounds | <https://www.legislation.gov.uk/ukpga/2006/1/contents> |
| Protection from Harassment Act 1997 | Creates harassment and stalking offences | <https://www.legislation.gov.uk/ukpga/1997/40/contents> |
| Protection of Children Act 1978 | Offences relating to indecent images of children | <https://www.legislation.gov.uk/ukpga/1978/37/contents> |
| Sexual Offences Act 2003 | Covers grooming, exploitation, and abuse of trust offences | <https://www.legislation.gov.uk/ukpga/2003/42/contents> |
| Public Order Act 1986 | Offences relating to racial hatred and public disorder | <https://www.legislation.gov.uk/ukpga/1986/64/contents> |
| Obscene Publications Acts 1959 & 1964 | Offences related to publishing obscene material | <https://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents> |
| Human Rights Act 1998 | Protects rights such as privacy and freedom of expression | <https://www.legislation.gov.uk/ukpga/1998/42/contents> |
| Education and Inspections Act 2006 | Pupil behaviour regulation, including off-site behaviour | <https://www.legislation.gov.uk/ukpga/2006/40/contents> |
| Education Act 2011 | Includes staff powers to search/confiscate electronic devices | <https://www.legislation.gov.uk/ukpga/2011/21/contents/enacted> |
| Protection of Freedoms Act 2012 | Covers biometrics in schools and safeguarding freedoms | <https://www.legislation.gov.uk/ukpga/2012/9/contents/enacted> |
| Education and Training (Welfare of Children) Act 2021 | Extends safeguarding duties to 16–19 providers | <https://www.legislation.gov.uk/ukpga/2021/15/contents/enacted> |
| Serious Crime Act 2015 | Created offence of sexual communication with a child | <https://www.legislation.gov.uk/ukpga/2015/9/contents/enacted> |
| Criminal Justice and Courts Act 2015 | Criminalises non-consensual sharing of intimate images (‘revenge porn’) | <https://www.legislation.gov.uk/ukpga/2015/2/contents/enacted> |
| Equality Act 2010 | Prohibits discrimination and harassment, including online | <https://www.legislation.gov.uk/ukpga/2010/15/contents> |
| Counter-Terrorism and Security Act 2015 (Prevent Duty) | Places duty on schools to prevent radicalisation online | <https://www.legislation.gov.uk/ukpga/2015/6/contents/enacted> |
| Online Safety Act 2023 | Introduces duties on platforms and supports online safety in education | <https://www.legislation.gov.uk/ukpga/2023/50/contents/enacted> |

# Appendix E – Key Organisations & Resources

• UK Safer Internet Centre – <https://www.saferinternet.org.uk/>

• South West Grid for Learning (SWGfL) – <https://swgfl.org.uk/products-services/online-safety/>

• Childnet – <https://www.childnet.com/>

• Professionals Online Safety Helpline – <https://www.saferinternet.org.uk/helpline>

• Revenge Porn Helpline – <https://revengepornhelpline.org.uk/>

• Internet Watch Foundation – <https://www.iwf.org.uk/>

• Report Harmful Content – <https://reportharmfulcontent.com/>

• CEOP (Child Exploitation & Online Protection) – <https://www.ceop.police.uk/>

• ThinkUKnow – <https://www.thinkuknow.co.uk/>

• UK Council for Internet Safety (UKCIS) – <https://www.gov.uk/government/organisations/uk-council-for-internet-safety>

• Online Safety BOOST (SWGfL) – <https://boost.swgfl.org.uk/>

• 360 Safe (self-review tool) – <https://360safe.org.uk/>

• ICO for Schools – <https://ico.org.uk/for-organisations/education/>

• NSPCC Learning – Photographing/filming children – <https://learning.nspcc.org.uk/online-safety/photographing-filming-children>

• UKCIS Education for a Connected World – <https://www.gov.uk/government/publications/education-for-a-connected-world>

**Glossary of Terms**

**AUP/AUA** Acceptable Use Policy/Agreement – see templates earlier in this document

**CEOP** Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse)

**CPD** Continuous Professional Development

**FOSI** Family Online Safety Institute

**ICO** Information Commissioners Office

**ICT** Information and Communications Technology

**INSET** In Service Education and Training

**IP address** The label that identifies each computer to other computers using the IP (internet protocol)

**ISP** Internet Service Provider

**ISPA** Internet Service Providers’ Association

**IWF** Internet Watch Foundation

**LA** Local Authority

**LAN** Local Area Network

**MAT** Multi Academy Trust

**MIS** Management Information System

**NEN** National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.

55

**Ofcom** Office of Communications (Independent communications sector regulator)

**SWGfL** South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW

**TUK** Think U Know – educational online safety programmes for schools, young people and parents.

**UKSIC** UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

**UKCIS** UK Council for Internet Safety

**VLE** Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

**WAP** Wireless Application Protocol

56

54

57

A more comprehensive glossary can be found at the end of the UKCIS [Education for a Connected World Framework](https://www.gov.uk/government/publications/education-for-a-connected-world)

1. [↑](#footnote-ref-1)