



ORWELL PARK SCHOOL

Online Safety Policy

This policy applies to all members of Orwell Park community (including staff, pupils, volunteers, parents and guardians, visitors, community users) who have access to and are users of school digital systems, both in and out of Orwell Park. It also applies to the use of personal digital technology on Orwell Park site (where allowed).

Date: 14/11/25

Next review date: 14/11/26

ONLINE SAFETY POLICY 0

SCOPE OF THE ONLINE SAFETY POLICY 2

POLICY AND LEADERSHIP 3

THE USE OF ARTIFICIAL INTELLIGENCE (AI) SYSTEMS IN SCHOOL..... 11

TECHNOLOGY 15

OUTCOMES 23

ORWELL PARK ONLINE SAFETY POLICY APPENDICES 25

APPENDIX A1- PUPIL ACCEPTABLE USE AGREEMENT TEMPLATE – FOR PUPILS IN YEAR 7 & 8 26

APPENDIX A2 - PUPIL ACCEPTABLE USE AGREEMENT TEMPLATE – FOR PUPILS IN YEAR 3-6 27

A4 PARENT/GUARDIAN ACCEPTABLE USE AGREEMENT TEMPLATE..... 30

A5 STAFF (AND VOLUNTEER) ACCEPTABLE USE AGREEMENT TEMPLATE..... 33

A6 LEGISLATION 36

A7 LINKS TO OTHER ORGANISATIONS OR DOCUMENTS..... 41

A8 GLOSSARY OF TERMS 44

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Orwell Park School to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Online Safety Policy applies to all members of Orwell Park community (including staff, pupils, governors, volunteers, parents and guardians, visitors, community users) who have access to and are users of school digital systems, both in and out of Orwell Park. It also applies to the use of personal digital technology on Orwell Park site (where allowed).

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

This Online Safety Policy has been developed by in collaboration with the following:

- *Head / SLT*
- *Designated safeguarding lead (DSL)*
- *Online Safety Leads (OSL)*
- *staff (including teachers/support staff/technical staff)*
- *governors*
- *parents and guardians*
- *community users*

Orwell Park will monitor the impact of the policy using:

- *logs of reported incidents*
- *Filtering and monitoring logs*
- *internal monitoring data for network activity*
- *surveys/questionnaires of:*
 - *pupils*
 - *parents and guardians*
 - *staff.*

Oversight of Online Safety takes place in the Pastoral, Safeguarding & Wellbeing Sub-Committee.

Policy and leadership

Summary of Responsibilities

Online safety at Orwell Park is a **shared responsibility**. Everyone in the community — from staff and governors to pupils and parents — plays a part in protecting pupils online, promoting responsible behaviour, and reporting concerns promptly.

Key Roles and Responsibilities (Summary)

Head

- Overall duty of care for safety and safeguarding culture.
- Ensures DSL and Online Safety Leads are trained and effective.
- Oversees procedures for responding to serious online safety allegations.
- Works with DSL, Online Safety Leads, Governors, and IT providers on filtering and monitoring systems.

Governors

- Approve and review the Online Safety Policy.
- Appoint and support the DSL.
- Monitor online safety incidents, training, and filtering standards.
- Ensure compliance with DfE safeguarding, filtering, and cyber-security standards.

Designated Safeguarding Lead (DSL)

- Holds overall responsibility for online safety within safeguarding.
- Leads incident response and reporting.
- Meets regularly with Online Safety Governor.
- Liaises with staff, IT providers, and external agencies.
- Receives ongoing training in online safety risks and procedures.

Online Safety Lead (OSL)

- Supports the DSL in all online safety matters.
- Promotes awareness and training for staff, pupils, and parents.
- Leads curriculum planning for online safety.
- Monitors incidents and trends.
- Works with IT, pastoral, and teaching staff.

Head of Digital & Life Skills

- Embeds online safety in lessons (Digital Skills, Life Skills/PHSE, assemblies, events).
- Promotes initiatives such as Safer Internet Day and Anti-Bullying Week.

Teaching & Support Staff

- Model safe and professional online behaviour.
- Follow safeguarding and GDPR guidance.
- Report concerns immediately to DSL.
- Embed online safety in teaching.
- Use technology and AI responsibly and transparently.

IT Provider / Head of Digital Services

- Maintain secure systems and filtering/monitoring tools.
- Provide reports and reviews on technical safety.
- Work with DSL and SLT to assess risks and update systems.
- Follow school online safety and security policies.

Pupils

- Follow the Online Safety Policy and code of conduct.
- Report concerns or inappropriate content.
- Use technology responsibly in and out of school.
- Avoid plagiarism and use AI safely.

Parents / Guardians

- Reinforce safe online behaviour at home.
- Engage with online safety education and updates from school.
- Support school policies and digital permissions.

Community Users

- Must sign the Acceptable Use Agreement before accessing school systems.

Online Safety Team

- Oversees online safety strategy and monitoring.
- Includes DSL, OSL, IT staff, Governors, and Pastoral representatives.
- Reviews policy, incidents, and education provision.
- Consults stakeholders and promotes improvement.

Overview Table

Role / Group	Core Responsibilities	Works With
Head	Ensures culture of online safety; oversees DSL, training, and monitoring systems; manages serious incidents.	DSL, OSL, Governors, IT Provider
Governors	Approve/review policy; monitor compliance; ensure DSL role and systems meet DfE standards.	Head, DSL, OSL
DSL (Designated Safeguarding Lead)	Leads on safeguarding and online safety; handles incidents; reports to SLT/Governors; liaises with staff and IT.	OSL, Head, IT Provider, Governor
OSL (Online Safety Lead)	Supports DSL; promotes education/training; reviews incidents; leads policy updates.	DSL, Teaching Staff, IT Provider
Head of Digital & Life Skills	Integrates online safety into curriculum and events.	DSL, OSL, Teachers
Teaching & Support Staff	Model safe behaviour; follow policy; teach online safety; report concerns; use AI responsibly.	DSL Team, Pupils
IT Provider / Head of Digital Services	Maintain filtering & monitoring; secure systems; provide reports; support reviews.	DSL, SLT, Head
Pupils	Use tech safely; report issues; follow rules; act responsibly online and offline.	Teachers, DSL
Parents / Guardians	Support safe use at home; engage with school's online safety education.	School Staff, Pupils
Community Users	Follow online safety agreements for access.	School Admin
Online Safety Team	Monitor and improve overall online safety strategy and policy.	DSL, OSL, IT, Governors

Staff at Orwell Park are expected to uphold the **same professional standards online** as in all aspects of school life:

- **Develop core skills:** Emphasise literacy, numeracy, digital competence, and digital resilience; support pupils in building these across the curriculum.

- **Use technology thoughtfully:** Apply new digital tools (including AI) in a structured, considered way; take care to manage associated risks.
- **Reflect and improve:** Review personal and collective practice against agreed standards; celebrate successes.
- **Follow official protocols:** Use only school-approved systems for online communication with staff, pupils, parents, and the wider community.

Online Safety Policy – Key Points

The policy at Orwell Park:

- **Sets expectations** for safe, responsible use of digital technologies in learning, administration, and communication.
- **Defines responsibilities** for implementing and maintaining online safety.
- **Is regularly reviewed** to reflect incidents, technology changes, and emerging behaviours.
- **Guides staff** on using digital tools responsibly to protect themselves, the school, and safeguard pupils.
- **Prepares pupils** to be safe and responsible online users.
- **Provides procedures** to identify, report, respond to, and record online safety incidents, including external support.
- **Includes related agreements** (Acceptable Use Agreements) for staff, pupils, and community users.
- **Is shared with staff** at induction and through regular communication.
- **Is published** on the Orwell Park website for wider access.

Acceptable Use

Orwell Park defines what is **acceptable and unacceptable** use of digital technologies through its **Online Safety Policy and Acceptable Use Agreements**.

Communication & Conduct

- All staff communication with pupils or parents must be **professional** and use **officially sanctioned school systems** (e-mail, learning platforms, etc.).
- Personal e-mails, text messages, or social media **must not** be used for official communication.
- Staff should follow good practice on **personal social media** to protect their own and the school's professional reputation.
- Users must **report immediately** any communication that is offensive, threatening, discriminatory, or bullying, and **not respond** to it.
- Online posting (school website, social media) must follow school policies; only school e-mail addresses should identify staff and pupils.

Reinforcement & Education

- Pupils: prep diaries, first Digital Skills lesson, education sessions.
- Staff: induction, handbook, September annual declarations.

- Visible reminders: posters and notices where technology is used.
- Parents/guardians: communicated through school channels.

Reporting and Responding to Online Safety Incidents

Orwell Park recognises that online safety incidents may occur both inside and outside school. The school follows clear procedures to respond effectively, protect pupils and staff, and learn from incidents.

Key Principles

- **Clear reporting routes:** All members of the school community know how to report concerns; aligned with safeguarding, whistleblowing, complaints, and staff misconduct procedures.
- **Prompt action:** Reports are dealt with as quickly as possible.
- **Trained staff:** DSL, Online Safety Lead, and other responsible staff have the skills to handle online safety risks.
- **Escalation of serious issues:** Suspected illegal activity or serious harm (e.g., child sexual abuse material, cybercrime, extremism, harassment, fraud, copyright infringement) is escalated through safeguarding procedures.
- **Staff misuse:** Reported to the Head; if the Head is involved, report to Chair of Governors and Local Authority.

Investigation Procedures (Non-Illegal Activity)

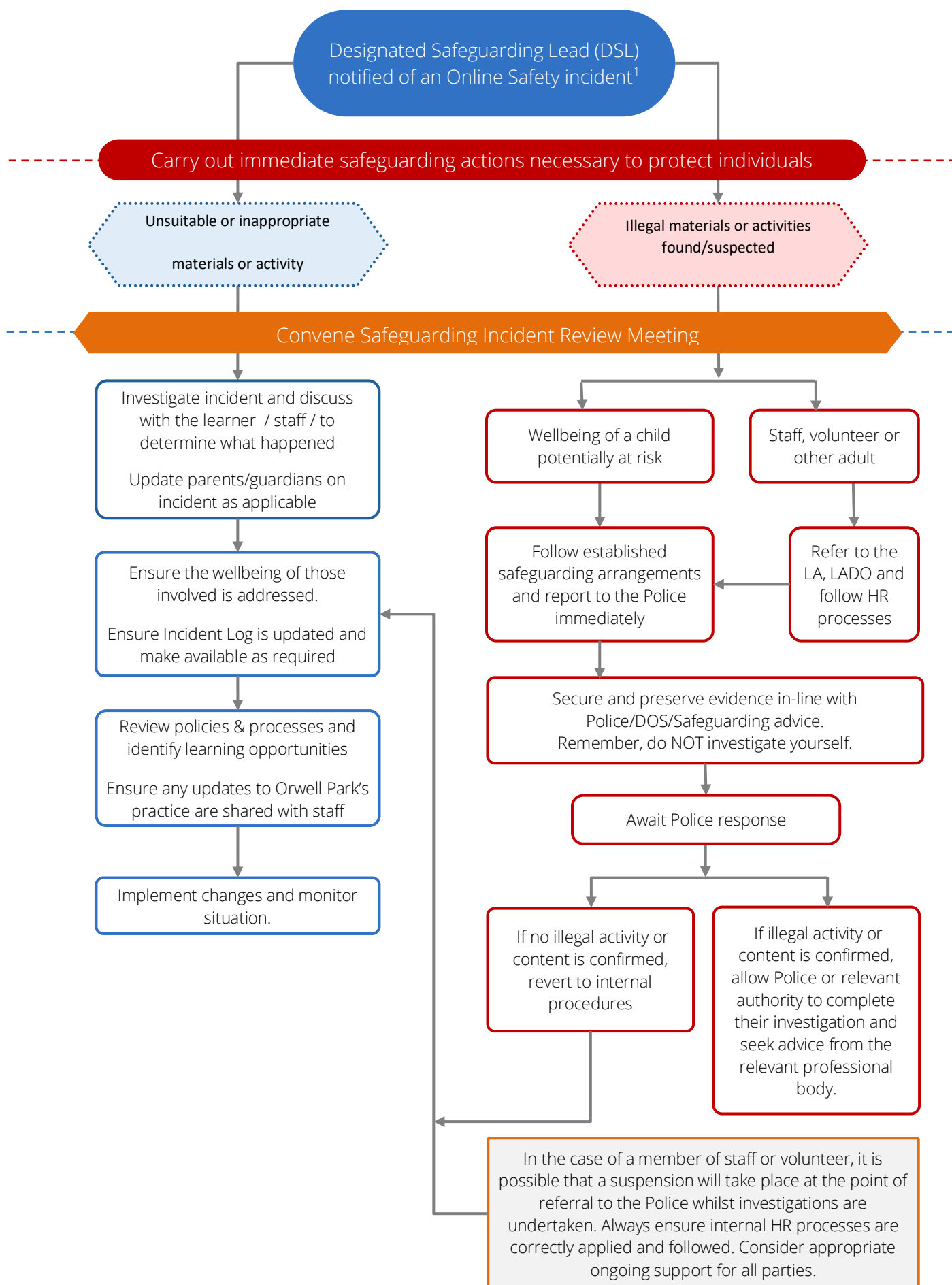
- Conducted by senior staff using a designated device.
- Internet activity is closely monitored and recorded.
- Evidence (URLs, screenshots) is collected securely.
- After investigation, appropriate action is taken: internal discipline, local authority, or police involvement.

Logging and Feedback

- Incidents are logged in the **Online Safety Log** and/or **MyConcern**.
- Staff, pupils, parents, governors, and external agencies are informed of outcomes as appropriate.
- Support is provided for those affected (e.g., peer support, safeguarding guidance).

Learning and Prevention

- Patterns of incidents are analysed to prevent future issues.
- Anonymous learnings inform:
 - Policy updates
 - Education programmes
 - Staff briefings
 - Pupil lessons/assemblies
 - Parent communications



Responding to & Reporting Online Misuse

Orwell Park deals mostly with inappropriate rather than illegal misuse of digital technologies. But have the following protocols in place to ensure that all incidents are handled quickly, proportionately, and transparently, and those involved are informed that the matter has been addressed.

General Approach

- **Pupils:** Most incidents are addressed through normal behaviour and disciplinary procedures.
- **Staff:** Incidents are addressed through line management, the Head, disciplinary procedures, and, if necessary, external authorities.
- **Serious incidents:** Illegal activity, repeated breaches, or actions that could seriously harm pupils, staff, or the school's reputation are escalated to DSL, police, or local authority as appropriate.

Pupil Misuse – Typical Actions

Type of Incident	Actions / Sanctions
Deliberately accessing illegal material	Tutor, Head of Section, MyConcern log, report to Deputy Head / Online Safety Lead, refer to Head, DSL/police if needed, inform parents, device removal, warning, reflection session, re-sign code of conduct
Attempting to access another user's account	Tutor, Head of Section, report to Deputy Head, inform parents, device removal, warning, reflection
Corrupting or destroying others' data	Tutor, Head of Section, Deputy Head, Head, DSL, Local Authority IT support, inform parents, device removal, warning, reflection
Offensive, harassing, or bullying messages	Tutor, Head of Section, Deputy Head, Head, inform parents, device removal, warning, reflection
Accessing or attempting to access offensive/pornographic material	Tutor, Head of Section, Deputy Head, Head, inform parents, device removal, warning, reflection
Breaching copyright / data protection	Tutor, Head of Section, Deputy Head, inform parents, device removal, warning, reflection
Using devices / online services without permission	Tutor, Head of Section, Deputy Head, inform parents, device removal, warning, reflection
Bringing school into disrepute	Tutor, Head of Section, Deputy Head, Head, inform parents, device removal, warning, reflection

Type of Incident	Actions / Sanctions
Repeated infringements	Escalation to Head, Deputy Head, DSL as above; stronger sanctions may apply

Staff Misuse – Typical Actions

Type of Incident	Actions / Sanctions
Accessing illegal material	Refer to line manager, Head, DSL, police/local authority; disciplinary action
Accessing offensive/pornographic material	Refer to line manager, Head, DSL, police; warning or disciplinary action
Corrupting data / damaging equipment	Refer to line manager, Head, DSL, police, LA IT support; disciplinary action
Using proxy sites / bypassing filtering	Line manager, Head, technical support, warning
Sending offensive/bullying messages	Line manager, Head, DSL, police; disciplinary action
Breaching copyright, IP, or AI use rules	Line manager, Head; warning / disciplinary action
Sharing passwords / unauthorized network access	Line manager, Head; warning / disciplinary action
Using personal accounts to communicate with pupils	Line manager, Head, DSL; warning / disciplinary action
Careless use of personal data	Line manager, Head, DSL; warning / disciplinary action
Actions damaging professional reputation or school ethos	Line manager, Head; warning / disciplinary action
Repeated infringements	Escalated to Head, DSL, possible suspension, disciplinary action

Key Points

- **Proportionality:** Most issues are handled internally unless serious harm or illegal activity is suspected.
- **Transparency:** Those involved are informed and records are kept.
- **Escalation:** Serious or repeated breaches involve DSL, Head, governors, police, or local authority as required.
- **Education:** Reflection sessions, warnings, and re-signing of the online code of conduct (Acceptable Use agreement) help reinforce safe and responsible online behaviour.

The use of Artificial Intelligence (AI) systems in School

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks.

We will educate staff and pupils about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

The safeguarding of staff and pupils will, as always, be at the forefront of our policy and practice.

Policy Statements

- Orwell Park acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and pupils for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR
- We will provide relevant training in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- We will seek to embed learning about AI as appropriate in our curriculum offer, including supporting pupils to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. Orwell Park recognises the importance of equipping pupils with the knowledge, skills and strategies to engage responsibly with AI tools.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.
- Orwell Park will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the pupils, being used to train generative AI models without appropriate consent.

- incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
- We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.

Online Safety Education Programme

While regulation and technical solutions are particularly important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of Orwell Park's online safety provision. Pupils need the help and support of Orwell Park to recognise and avoid online safety risks and develop their resilience.

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for:

"a carefully sequenced RSHE curriculum, based on the Department for Education's (DfE's) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of 'nudes'."

Keeping Children Safe in Education states:

"Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum ..."

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:

There is a planned online safety curriculum delivered through Life Skills & Digital Skills.

- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; RSE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. [Safer Internet Day](#) and [Anti-bullying week](#)
- the programme will be accessible to pupils at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- pupils are taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information (including where the information is gained from Artificial Intelligence services)

- pupils should be taught to acknowledge the source of information used and to respect copyright / intellectual property when using material accessed on the internet and particularly through the use of Artificial Intelligence services
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- pupils are helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the [CyberChoices](#) site.
- staff 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 are vigilant in supervising the pupils and monitoring the content of the websites / tools (including AI systems) the pupils visit
- it is accepted that from time to time, for good educational reasons, pupils may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable. This should be done via email request to Head of Digital Services, Rob Brown (Sept 2025), with clear reasons for the need.

Contribution of Pupils

Orwell Park acknowledges, learns from, and uses the skills and knowledge of pupils in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for Orwell Park community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- *mechanisms to canvass pupil feedback and opinion.*
- *the Online Safety Team gathers pupil data and opinions to inform policy and practice*
- *pupils contribute to the online safety education programme and online safety campaigns*
- *pupils contribute to designing/updating acceptable use agreements (in Digital Skills' Lessons)*

Staff/volunteers

The DfE guidance "[Keeping Children Safe in Education](#)" states:

"All staff should receive appropriate safeguarding and child protection training (**including online safety**) at induction. The training should be **regularly updated**. In addition, all staff should receive safeguarding and child protection (**including online safety**) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively."

“Governing bodies and proprietors should ensure... that safeguarding training for staff, **including online safety** training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning.”

All staff will 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 and data protection training will be made available to all staff. This will be regularly updated and reinforced.
- the training will be an integral part of Orwell Park’s annual safeguarding, data protection and cyber-security training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand Orwell Park online safety policy and acceptable use agreements (‘Staff Online and Technology Code of Conduct’). It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- the Online Safety Leads and Designated Safeguarding Lead will receive regular updates through attendance at external training events such as Suffolk Safeguarding Partnership 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/INSET days
- the Designated Safeguarding Lead &/Online Safety Leads will provide advice/guidance/training to individuals as required.

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. (Sub Committee: Pastoral, Safeguarding & Wellbeing).

This may be offered in several ways such as:

- attendance at training provided by the local authority or through AGBIS or other relevant organisation (e.g., SWGfL)
- participation in school training / information sessions for staff or parents
- induction or annual Governing body update from the DSL
- online training and courses

A higher level of training will be made available to (at least) the Online Safety Governor. This will include:

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand Orwell Park’s filtering and monitoring provision, in order that they can participate in the required checks and reviews.

Families

Many parents and guardians 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.

Orwell Park will seek to provide information and awareness to parents and guardians through:

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/guardians on online safety issues through monthly updates in the OrWellbeing Newsletter and / or awareness workshops
- the pupils – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by pupils leading sessions at parent/carer evenings.
- high profile events / campaigns e.g. [Safer Internet Day](#)
- reference to the relevant web sites/publications, e.g. [SWGfL](#); www.saferinternet.org.uk/; www.childnet.com/parents-and-guardians (see Appendix for further links/resources).

Technology

Orwell Park is responsible for ensuring that Orwell Park infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Orwell Park should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Filtering & Monitoring

The DfE guidance (for England) on filtering and monitoring in “[Keeping Children Safe in Education](#)” states:

“It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children’s exposure to the ... risks from Orwell Park’s or college’s IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified...”

The Department for Education has published [filtering and monitoring standards](#) to support schools in this process.

Orwell Park’s filtering and monitoring provision is agreed by the Senior Leadership Team, governors and the Head of Digital Services & the Online Safety Leads and is regularly reviewed (at least annually). It is updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the Head of Digital Services will have technical responsibility the filtering and monitoring provision is reviewed (at least annually) by Senior Leadership Team, the Designated Safeguarding Lead and a governor with the involvement of the Head of Digital Service.

- checks on the filtering and monitoring system are carried out by the Head of Digital Services (Technical and Head of Digital Skills (Teaching) with the involvement of a senior leader, the Designated Safeguarding Lead and with governor oversight, in particular when a safeguarding risk is identified,

there is a change in working practice, e.g. remote access or BYOD or new technology is introduced
e.g. using [SWGfL Test Filtering](#)

Filtering

The DfE Technical Standards for Schools and Colleges states:

“Schools and colleges have a statutory responsibility to keep children and young people safe online as well as offline. Governing bodies and proprietors should make sure their school or college has appropriate filtering and monitoring systems in place, as detailed in the statutory guidance, Keeping children safe in education.

Filtering is preventative. It refers to solutions that protect users from accessing illegal, inappropriate and potentially harmful content online. It does this by identifying and blocking specific web links and web content in the form of text, images, audio and video

These standards help school and college leaders, designated safeguarding leads and IT support understand how to work together to make sure they can effectively safeguard their students and staff.”

- Orwell Park manages access to content across its systems for all users and on all devices using Orwell Parks internet provision. The filtering provided meets the standards defined in the DfE [Filtering standards for schools and colleges](#) and the guidance provided in the UK Safer Internet Centre [Appropriate filtering](#).
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures. Staff should report without to delay to the Head of Digital Services and the Online Safety Leads.
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- There are regular checks of the effectiveness of the filtering systems. Checks are undertaken across a range of devices at least termly and the results recorded and analysed to inform and improve provision. The DSL and Governor are involved in the process and aware of the findings. [\(Schools may wish to use e.g. using SWGfL Testfiltering.com to carry out these checks\)](#)
- Devices that are provided by Orwell Park have school-based filtering applied irrespective of their location.
- Orwell Park has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/pupils, etc.)
- Orwell Park has a mobile phone policy and where personal mobile devices have internet access through Orwell Park network, content is managed in ways that are consistent with school policy and practice.
- If necessary, Orwell Park will seek advice from, and report issues to, the SWGfL [Report Harmful Content](#) site.

Monitoring

The DfE Technical Standards for Schools and Colleges states:

“Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity. Monitoring can be manual, for example, teachers viewing screens as they walk around a classroom. Technical monitoring solutions rely on software applied to a device that views a user’s activity. Reports or alerts are generated based on illegal, inappropriate, or potentially harmful activities, including bullying. Monitoring solutions do not block users from seeing or doing anything.”

Orwell Park follows the UK Safer Internet Centre [Appropriate Monitoring](#) guidance.

Orwell Park has monitoring systems in place, agreed by Senior Leadership Team and the Head of Digital Services, to protect the school, systems and users:

Orwell Park monitors all network use across all its devices and services.

- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead and Online Safety Leads. All users are aware that monitoring is in place.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review is completed by the Online Safety Leads (which includes the Head of Digital Services and the DSL, a member of the SLT). The results of the review will be recorded and reported as relevant.
- Devices that are provided by Orwell Park have school-based monitoring applied irrespective of their location.
- monitoring enables alerts to be matched to users and devices.
- where AI –supported monitoring is used, the purpose and scope of this is clearly communicated

Orwell Park technical systems will be managed in ways that ensure that Orwell Park meets recommended standards in the [DfE Technical Standards for Schools and Colleges](#)

Responsibility for technical security resides with SLT who may delegate activities to identified roles.

- An access control model is in place, clearly defining access rights to school systems and devices. This is reviewed annually. All users (staff and pupils) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
- password policy and procedures are implemented and are consistent with guidance from the National Cyber Security Centre
- all school networks, devices and system will be protected by secure passwords.. ([see section on passwords in ‘Technical security policy template’ in the Appendix C1](#))
- the administrator passwords for school systems are kept in a secure place
- there is a risk-based approach to the allocation of learner usernames and passwords. ([see ‘Technical security policy template’ in the Appendix C1 for more information](#))
- there will be regular reviews and audits of the safety and security of school technical systems

- servers, wireless systems and cabling are securely located and physical access restricted
- appropriate security measures are in place (schools may wish to provide more detail which may need to be provided by the service provider) to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of Orwell Park systems and data. These are tested regularly. Orwell Park infrastructure and individual workstations are protected by up-to-date endpoint software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,

The Head of Digital Services is responsible for ensuring that all software purchased by and used by Orwell Park is adequately licenced and that the latest software updates (patches) are applied.

- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on Orwell Park network is regulated by acceptable use statements that a user consents to when using the network
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/Head of Digital Services
- systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- mobile device security and management procedures are in place (where mobile devices are allowed access to school systems). (Schools may wish to add details of the mobile device security procedures that are in use).
- guest users are provided with appropriate access to school systems based on an identified risk profile.
- Care will be taken when using Artificial Intelligence services to avoid the input of sensitive information, such as personal data, internal documents or strategic plans, into third-party AI systems unless explicitly vetted for that purpose. Staff must always recognise and safeguard sensitive data.
- dual-factor authentication is used for sensitive data or access outside of a trusted network

Mobile technologies

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

“The School or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.

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

All users should understand that the primary purpose of the use of mobile/personal devices in a school context at Orwell Park is either for **communication** with home in the boarding house or **educational**.

Orwell Park acceptable use agreements for staff, pupils, parents, and guardians outline the expectations around the use of mobile technologies.

Orwell Park allows:

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised device ¹	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes (Boarders only)	Yes	Yes
Full network access	Yes	Yes	Yes	Yes	Yes	No
Internet only						Yes (Guest Wifi Access)
No network access						

School owned/provided devices:

- all school devices are managed through the use of Mobile Device Management software
- there is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed
- the use of devices on trips/events away from school is clearly defined and expectations are well-communicated
- education is in place to support responsible use.

Personal devices:

- there is a clear policy covering the use of personal mobile devices on school premises for all users (See Orwell Park Online & Technology Code of Conduct)
- where devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all pupils can access a required resource.

¹ Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by Orwell Park.

- where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storage should be made available. For example, in Early Years, we have locked storage facilities in the staffroom for personal devices.
- taking/storing/using images/video on personal devices is not allowed. School devices must be used and procedures must align with Orwell Park's acceptable use policy. The non-consensual taking/using of images of others is not permitted.
- education about the safe and responsible use of mobile devices is included in Orwell Park online safety education programmes

Social media

With widespread use of social media for professional and personal purposes this policy that sets out clear guidance for staff to manage risk and behaviour online.

Expectations for teachers' professional conduct are set out in the DfE Teachers Standards, Independent School Regulations and Keeping Children Safe in Education but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

Orwell Park provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils through:

- ensuring that personal information is not published.
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- clear reporting guidance, including responsibilities, procedures, and sanctions.
- risk assessment, including legal risk.
- guidance for pupils, parents/guardians

School staff should ensure that:

- No reference should be made in their personal social media to pupils, parents/guardians or school staff.
- they do not engage in online discussion on personal matters relating to members of Orwell Park community.
- personal opinions should not be attributed to Orwell Park.
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- they act as positive role models in their use of social media

Orwell Park's official school social media accounts are:

- approved by the Senior Leadership Team
- have clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- 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, or impacts on, Orwell Park it must be made clear that the member of staff is not communicating on behalf of Orwell Park with an appropriate disclaimer. Such personal communications are within the scope of this policy
- personal communications which do not refer to or impact upon Orwell Park 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
- Orwell Park permits reasonable and appropriate access to personal social media sites during school hours and understands that many staff live in school and school hours are 24 hours a day.

Monitoring of public social media

- As part of active social media engagement, Orwell Park may pro-actively monitor the Internet for public postings about Orwell Park.
- Orwell Park should effectively respond to social media comments made by others according to a defined policy or process.
- when parents/guardians express concerns about Orwell Park on social media we will urge them to make direct contact with Orwell Park, in private, to resolve the matter. Where this cannot be resolved, parents/guardians should be informed of Orwell Park complaints procedure.

School use of social media for professional purposes will be checked regularly by the DSL, Head and Online Safety Leads to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that Orwell Park is unable to resolve support may be sought from the Professionals Online Safety Helpline.

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/guardians 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.

Orwell Park will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm

- Orwell Park may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- when using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those pupils whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should never be used for

such purposes. If staff are unsure of photographic permissions, they should speak to the Head of Marketing or review the up-to-date photo permissions list kept by the Head of Marketing.

- in accordance with [guidance from the Information Commissioner's Office](#), parents/guardians are welcome to take videos and digital images of their children at school events for their own personal use (as such use is 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/guardians comment on any activities involving other pupils in the digital/video images**
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that pupils are appropriately dressed
- 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 Online Safety Policy
- **pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.**
- **permission from parents or guardians will be obtained before photographs of pupils are taken for use in school or published on Orwell Park website/social media.** (Permission is not required for images taken solely for internal purposes.)
- **parents/guardians will be informed of the purposes for the use of images, how they will be stored and for how long**
- images will be securely stored
- pupils' work can only be published with the permission of the learner and parents/guardians.

Online Publishing

Orwell Park communicates with parents/guardians and the wider community and promotes Orwell Park through:

- Public-facing website
- Social media
- Online newsletters

Orwell Park ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of pupils / previous pupils, publication of school calendars and personal information – ensuring that there is least risk to members of Orwell Park community, through such publications.

Where pupil work, images or videos are published, their identities are protected, and full names are not published.

Cyber Security (new January 2025)

[The DfE Cyber security standards for schools and colleges explains:](#)

“Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside Orwell Park or college and can lead to:

- safeguarding issues due to sensitive personal data being compromised
- impact on student outcomes
- a significant data breach
- significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including school or college closure
- financial loss
- reputational damage”

The ‘Cyber-security in schools: questions for governing bodies and Trustees’ guidance produced by the National Cyber Security Centre (NCSC) aims to support governing bodies’ and management committees’ understanding of their education settings’ cyber security risks. The guidance includes eight questions to facilitate the cyber security conversation between the governing body and school leaders, with the governing body taking the lead.

- Orwell Park has reviewed the DfE Cyber security standards for schools and colleges and is working toward meeting these standards.
- Orwell Park will conduct a cyber risk assessment annually and review each term
- Orwell Park, (*in partnership with their technology support partner*), has identified the most critical parts of Orwell Park’s digital and technology services and sought assurance about their cyber security
- Orwell Park has an effective backup and restoration plan in place in the event of cyber attacks
- Orwell Park’s governance and IT policies reflect the importance of good cyber security
- staff and Governors receive training on the common cyber security threats and incidents that schools experience
- Orwell Park’s education programmes include cyber awareness for pupils
- Orwell Park has a business continuity and incident management plan in place
- there are processes in place for the reporting of cyber incidents. All students and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this feel safe and comfortable to do so.

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, pupils; parents/guardians and is reported to Pastoral, Safeguarding & Wellbeing Sub-Committee on a termly basis:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors

- parents/guardians are informed of patterns of online safety incidents as part of Orwell Park's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Orwell Park Online Safety Policy

Appendices

Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be found in the links and resources section of the relevant aspects in the 360safe self-review tool and online on the [SWGfL website](#). The appendices are as follows:

- A1 - Learner Acceptable Use Agreement Template – for older pupils
- A2 - Learner Acceptable Use Agreement Template – KS2
- A3 - LEARNER ACCEPTABLE USE AGREEMENT TEMPLATE – FOR YOUNGER PUPILS (FOUNDATION/KS1)
- A4 - PARENT/CARER ACCEPTABLE USE AGREEMENT TEMPLATE
- A5 - STAFF (AND VOLUNTEER) ACCEPTABLE USE POLICY AGREEMENT TEMPLATE
- A6 - LEGISLATION
- A7 - Links to other organisations and resources
- A8 - GLOSSARY OF TERMS

Appendix A I- Pupil Acceptable Use Agreement Template – for Pupils in Year 7 & 8

Pupil Acceptable Use Agreement Form

I agree to use Orwell Park's digital systems responsibly to protect my safety, the security of Orwell Park systems, and others.

Personal Safety

- Orwell Park will monitor my use of its digital systems, devices, and communications.
- I will keep my usernames and passwords secure and private. If compromised, I will report or change them immediately.
- I will only share personal information, like my name or address, when absolutely necessary and with permission.
- I will be cautious when meeting online contacts in person, only doing so with a trusted adult in a public place.
- I will take responsibility for my actions online, using tools like blocking or ending chats if needed.
- I will share images of myself or others only when it is safe and will ensure the images are appropriate and respectful.
- I will only take or share images of myself, or others, when fully dressed. I understand that sharing nude or semi-nude content can cause distress, may be illegal and could lead to prosecution / criminal records.
- I will report harmful or unpleasant material, messages, or anything that worries or upsets me to a trusted adult.

Respecting Others' Work and Information

- I will seek permission before using or adapting someone else's work.
- I will verify information I find online, as it may not always be accurate or truthful.
- I will only use Artificial Intelligence (AI) tools approved by Orwell Park and ensure my use is ethical, legal, and transparent.
- I will fact-check and critically evaluate AI-generated content for accuracy, bias, and discrimination before sharing or publishing.
- I will avoid downloading or using copyrighted or protected materials without proper permissions.

Responsible Online Behaviour

- 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 bully, harass, threaten, upset or make fun of others.

- I will only use platforms or software approved by Orwell Park and will not attempt to bypass the filtering/security systems in place. If I become aware of any such attempts, I will report this to a trusted adult.
- I understand cybersecurity poses a risk to both me, other pupils and Orwell Park and will ensure I take precautions before accessing emails, messages or links. I will check with trusted adults if I have any such concerns.
- I will immediately report any damage, faults or failings involving equipment or software, however this may have happened.
- I will follow the age requirements for social media, apps, and tools.
- I will balance my online and offline activities to promote a healthy lifestyle.
- I will protect my online reputation and that of Orwell Park, its staff, and other pupils.
- I understand that some online behaviours might be regarded, by some, as fun but can have serious consequences – this might include taking (or sharing) images/videos of staff, fights, pupils in embarrassing situations or the setting up of fake accounts.
- I will ensure my behaviour reflects positively on Orwell Park, both in and out of school settings.

Consequences of Misuse

- I understand that failing to follow this agreement may lead to consequences, including loss of access to Orwell Park's systems, detentions, suspensions, contacting parents/guardians, or involvement of the police in serious cases.

By following these guidelines, I will contribute to a safe, respectful, and productive online environment.

I have read and understand the above and agree to follow these guidelines when:

- I use Orwell Park's systems and devices (both in and out of school)
- I use my own devices in Orwell Park (when allowed)
- I use digital technologies out of Orwell Park in a way that is related to me being a member of this school e.g. communicating with other members of Orwell Park, accessing school email, website etc.

Name of Pupil: Group/Class:.....

Signed: Date:.....

Head of Digital Skills signed:

Appendix A2 - Pupil Acceptable Use Agreement Template – for Pupils in Year 3-6

Acceptable Use Agreement

I agree to use Orwell Park's digital systems safely and responsibly to protect me, other pupils and Orwell Park.

Keeping Safe Online

- Orwell Park will check how I use devices and the internet to keep everyone safe.
- I will keep my usernames and passwords private and tell a trusted adult if someone else knows them.
- I will be careful when talking to people online and will only talk to people I know and trust.
- I will not share personal information like my name, address, or photos without asking a trusted adult.
- I will only take or share images of myself, or others, when fully dressed.
- If I see or hear something online that worries or upsets me, I will tell a trusted adult straight away.
- I will only meet people I have spoken to online if a trusted adult is with me.

Using Computers and the Internet Sensibly

- I will only use devices, apps and sites that I am allowed to, and will check if I am unsure.
- I will always ask permission and check with a trusted adult before using someone else's work or pictures.
- I will make sure the information I find online is true by checking carefully.
- I will only use apps or tools, like AI, that my teacher has said are OK, and I will ask for help if I'm unsure.
- I will not copy or use music, videos, or games unless I have permission.
- I will tell a trusted adult about any damage to devices or if anything else goes wrong.
- I will check with trusted adults before clicking on any unexpected messages or links (even if these look as though they are from people that I already know).

Being Respectful and Responsible

- I will treat others kindly online, just as I do in real life.
- I will make good choices about what I share online to protect myself and others.
- I will spend a healthy amount of time using devices and make time for other activities too.
- I will always think about how my behaviour online could affect me, my friends, and my school.

What Happens If I Break These Rules

- If I don't follow these rules, my teacher may stop me from using computers or devices, speak to my parents, or take other actions to help me make better choices in the future.

By following these rules, I can enjoy using technology safely and responsibly.

I have read and understand the above and agree to follow these guidelines when:

- I use Orwell Park systems and devices (both in and out of school)
- I use my own devices in Orwell Park (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.

- I am out of school and involved in any online behaviour that might affect Orwell Park or other members of Orwell Park.

Name of Pupil: Group/Class:

Signed: Date:

Head of Digital Skills / Tutor signed:

A3 Pupil Acceptable Use Agreement Template – for younger pupils (Early Years / Pre-Prep)

We will have these rules up on the wall in our classrooms to help us remember. Our teachers will talk us through these often so we can remember them.

Our Technology Rules

I will follow these rules to use computers, tablets and the internet safely at school.

Staying Safe

- My teacher will watch what I do on computers, tablets and the internet to keep me safe.
- I will keep my passwords secret and tell my teacher if I need help.
- I understand that people online are not always who they say they are. I will only talk to people online if my teacher or a trusted adult says it's OK.
- I will not share my name, address, or pictures without asking my teacher or a trusted adult first.
- If I see something that makes me feel worried or upset, I will tell my teacher or a trusted adult straight away.
- I will only use apps, games or websites my teacher says are safe.

Using Technology Kindly

- I will be kind when using technology, just like I am in real life.
- I will take care of the computers and tablets I use.
- I will only look at things my teacher says are OK.

Making Good Choices

- I will ask my teacher before I use someone else's pictures or work.

- I will take breaks from screens and do other fun things too.
- I know that I can say no / please stop to anyone online who makes me feel sad, uncomfortable, embarrassed or upset.
- I will ask for help from a trusted adult if I am not sure what to do or if I think I may have done something wrong.

What Happens If I Forget the Rules

- If I forget the rules, my teacher will help me learn to make better choices next time.

These rules help us all stay safe and have fun using computers and tablets at school!

A4 Parent/Guardian Acceptable Use Agreement Template

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 have an entitlement to safe internet access at all times.

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 guardians 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.

Orwell Park will try to ensure that pupils 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 learner acceptable use agreement is attached to this permission form, so that parents/guardians will be aware of Orwell Park expectations of the young people in their care.

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

Permission Form

Parent/Guardians Name:

Learner Name:

As the parent/guardian of the above pupils, I give permission for my son/daughter to have access to the digital technologies at school.

Either: (KS2 and above)

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.

Or: (KS1)

I understand that Orwell Park 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 Orwell Park 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 Orwell Park 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 Orwell Park 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 Orwell Park if I have concerns over my child's online safety.

Signed:

Date:

Use of Digital/Video Images

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 Orwell Park website and occasionally in the public media. Where an image is publicly shared by any means, only your child's first name will be used.

Orwell Park will comply with the Data Protection Act and request parent's/guardian's permission before taking images of members of Orwell Park. We will also ensure that when images are published that the pupils cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents/guardians are welcome to take videos and digital images of their children at school events for their own personal use (as such use is 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/guardians comment on any activities involving other pupils in the digital/video images.

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

Digital/Video Images Permission Form

Parent/Guardians Name:.....Learner Name:.....

As the parent/carers of the above learner, I agree to Orwell Park 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 Orwell Park.	Yes/No
Insert statements here that explicitly detail where images are published by Orwell Parks	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

Signed:

Date:

A5 Staff (and Volunteer) Acceptable Use Agreement Template

School Policy

Digital technologies have become integral to the lives of everyone, including children and young people, both within schools and in their lives outside school. The internet and digital technologies are powerful tools, which 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. Orwell Park has the right to protect itself and its systems and 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 online and using 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 users at risk
- that staff are protected from potential risk in their use of technology in their everyday work.

Orwell Park will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities 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 minimise the risk to the safety, privacy or security of Orwell Park community and its systems. I acknowledge the potential of digital technologies for enhancing learning and will endeavour to integrate them in a way that aligns with Orwell Park's policy, ethos and values.

For my professional and personal safety:

- I understand that Orwell Park will monitor my use of school devices and digital technology systems
- I understand that the rules set out in this agreement also apply to use of these devices and technologies out of school, and to the transfer of personal / sensitive data (digital or paper based) out of Orwell Park
- I understand that Orwell Park devices and digital technology systems are primarily intended for educational use and that I will only use them for personal or recreational use within relevant school policies.
- 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 will store my passwords securely and in line with Orwell Park's relevant security policy.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using digital technologies and 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 Orwell Park's policy on the use of digital/video images, and taking account of parental permissions. 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 Orwell Park website) 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 Orwell Park in accordance with school policies.
- I will only communicate with pupils and parents/guardians using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

Orwell Park has the responsibility to provide safe and secure access to technologies and ensure the smooth running of Orwell Park:

- I will abide by all relevant guidance and legislation (e.g., Keeping Children Safe in Education / UK GDPR)
- I will ensure that I am aware of cyber-security risks and that I will not respond to any communications that might put my / school data or systems at risk from attack
- When using AI systems in my professional role I will use these responsibly and:
 - will only use AI technologies approved by Orwell Park
 - will be aware of the risks of bias and discrimination, critically evaluating the outputs of AI systems for such risks
 - to protect personal and sensitive data, I will ensure that I have explicit authorisation when uploading sensitive school-related information into AI systems
 - will take care not to infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the pupils, being used to train generative AI models without appropriate consent.
 - ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance
 - critically evaluate AI-generated outputs to ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing
 - will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identity and well-being
- *When I use my personal mobile devices in school, I will follow the rules set out by Orwell Park, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus / anti-malware software and are free from viruses.*
- *When communicating in a professional capacity, I will only use technology and systems sanctioned by Orwell Park.*
- *I will not use personal accounts on school systems.*
- I will exercise informed safe and secure practice when accessing links to content from outside of my organisation to reduce the risk of cyber security threats.

- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not access illegal, inappropriate or harmful content on school systems.
- I will not bypass any filtering or security systems that are used to prevent access to such content.
- I will not install or attempt to install unauthorised programmes of any type on a school device , nor will I try to alter device settings, unless this is allowed in school policies
- 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 Orwell Park Data Security Policy (or other relevant 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 the data protection policy requires that any staff or learner 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.
- 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 appropriate permissions to use the original work of others in my own work and will reflect this with appropriate acknowledgements, particularly where AI has been used to generate content
- Where content is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of Orwell Park:

- I understand that this acceptable use agreement applies to my use of digital technologies related to my professional responsibilities , within or outside of Orwell Park.
- I will ensure my use of technologies and platforms is in line with Orwell Park's agreed codes of conduct.
- 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 Governors and/or the Local Authority in the event of illegal activities, the involvement of the Police.

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

Staff/Volunteer Name:

Signed:

Date:

A6 Legislation

Schools should be aware of the legislative framework under which this online safety policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

A useful summary of relevant legislation can be found at: [Report Harmful Content: Laws about harmful behaviours](#)

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Schools may wish to view the National Crime Agency website which includes information about [“Cyber crime – preventing young people from getting involved”](#). Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful [summary of the Act on the NCA site](#).

Data Protection Act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject’s rights.
- Secure.
- Not transferred to other countries without adequate protection.

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.

- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;

- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- Orwell Park reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct

causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In Orwell Park context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. Orwell Park is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Heads, to such extent as is reasonable, to regulate the behaviour of pupils when they are off Orwell Park site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Heads (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

(see template policy in these appendices and for DfE guidance -

<http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation>)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carers to use Biometric systems

Orwell Park Information Regulations 2012

Requires schools to publish certain information on its website:

<https://www.gov.uk/guidance/what-maintained-schools-must-publish-online>

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the [Revenge Porn Helpline](#)

A7 Links to Other Organisations or Documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

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

South West Grid for Learning - <https://swgfl.org.uk/products-services/online-safety/>

Childnet – <http://www.childnet-int.org/>

Professionals Online Safety Helpline - <http://www.saferinternet.org.uk/about/helpline>

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

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

Report Harmful Content - <https://reportharmfulcontent.com/>

[Harmful Sexual Support Service](#)

CEOP

CEOP - <http://ceop.police.uk/>

ThinkUKnow - <https://www.thinkuknow.co.uk/>

Others

LGfL – [Online Safety Resources](#)

Kent – [Online Safety Resources page](#)

INSAFE/Better Internet for Kids - <https://www.betterinternetforkids.eu/>

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

Tools for Schools / other organisations

Online Safety BOOST – <https://boost.swgfl.org.uk/>

360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

360Data – online data protection self-review tool: www.360data.org.uk

SWGfL Test filtering - <http://testfiltering.com/>

UKCIS Digital Resilience Framework - <https://www.gov.uk/government/publications/digital-resilience-framework>

[SWGfL 360 Groups](#) – online safety self review tool for organisations working with children

[SWGfL 360 Early Years](#) - online safety self review tool for early years organisations

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - <http://enable.eun.org/>

SELMA – Hacking Hate - <https://selma.swgfl.co.uk>

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government - Better relationships, better learning, better behaviour - <http://www.scotland.gov.uk/Publications/2013/03/7388>

DfE - Cyberbullying guidance -

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Heads_and_School_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit:

<http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit>

[Childnet – Project deSHAME – Online Sexual Harrassment](#)

[UKSIC – Sexting Resources](#)

Anti-Bullying Network – <http://www.antibullying.net/cyberbullying1.htm>

[Ditch the Label – Online Bullying Charity](#)

[Diana Award – Anti-Bullying Campaign](#)

Social Networking

Digizen – [Social Networking](#)

UKSIC - [Safety Features on Social Networks](#)

[Children's Commissioner, TES and Schillings – Young peoples' rights on social media](#)

Curriculum

SWGfL Evolve - <https://projectevolve.co.uk>

[UKCCIS – Education for a connected world framework](#)

Department for Education: Teaching Online Safety in Schools

Teach Today – www.teachtoday.eu/

Insafe - [Education Resources](#)

Data Protection

[360data - free questionnaire and data protection self review tool](#)

[ICO Guides for Organisations](#)

[IRMS - Records Management Toolkit for Schools](#)

[ICO Guidance on taking photos in schools](#)

Professional Standards/Staff Training

[DfE – Keeping Children Safe in Education](#)

DfE - [Safer Working Practice for Adults who Work with Children and Young People](#)

[Childnet – School Pack for Online Safety Awareness](#)

[UK Safer Internet Centre Professionals Online Safety Helpline](#)

Infrastructure/Technical Support/Cyber-security

[UKSIC – Appropriate Filtering and Monitoring](#)

[SWGfL Safety & Security Resources](#)

Somerset - [Questions for Technical Support](#)

SWGfL - [Cyber Security in Schools](#).

NCA – [Guide to the Computer Misuse Act](#)

NEN – [Advice and Guidance Notes](#)

Working with parents and guardians

[SWGfL – Online Safety Guidance for Parents & Guardians](#)

[Vodafone Digital Parents Magazine](#)

[Childnet Webpages for Parents & Guardians](#)

[Get Safe Online - resources for parents](#)

[Teach Today - resources for parents workshops/education](#)

[Internet Matters](#)

Prevent

[Prevent Duty Guidance](#)

[Prevent for schools – teaching resources](#)

Childnet – [Trust Me](#)

Research

[Ofcom –Media Literacy Research](#)

Ofsted: Review of sexual abuse in schools and colleges

Further links can be found at the end of the UKCIS [Education for a Connected World Framework](#)

A8 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, providers of the Think U Know programmes.
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.
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

A more comprehensive glossary can be found at the end of the UKCIS [Education for a Connected World Framework](#)

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in January 2025. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.

© SWGfL 2025