IPSWICH SCHOOL

ONLINE SAFETY POLICY

Scope of the Policy

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

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

Ipswich 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.

Roles and Responsibilities

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

Head:

The Head has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety is delegated to the DSL and Online Safety Lead.

Designated Safeguarding Lead

The Designated Safeguarding Lead (DSL) is trained in Online Safety issues and is aware of the potential for serious child protection/safeguarding issues to arise from:

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

The DSL has responsibility for addressing any issues that arise from the filtering and monitoring reports created by the technical staff.

Online Safety Lead:
The Online Safety Lead takes day-to-day responsibility for online safety issues and helps in establishing and reviewing the school online safety policies/documents. Other responsibilities include:

- Ensuring all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Lead sessions on staff training at appropriate intervals.
- Liaising with school technical staff.
- Reports regularly to the DSL.

IT Director and technical team:
The Director of IT and technical team is responsible for ensuring:

- that the School's technical infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the networks and devices through a properly enforced password protection policy
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role
- that the use of the network/internet/email/Google suite of apps is monitored when there has been suspected misuse/attempted misuse and reported to the Head/Senior Leader for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in Ipswich School policies.

Teaching and Support Staff:
Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current Ipswich School Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the Head/Senior Leader for investigation/action/sanction
- all digital communications with pupils/parents/guardians should be on a professional level and only carried out using official school systems
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons, where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils:

- are responsible for using the Ipswich School digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that Ipswich School's Online Safety Policy covers their actions out of school, if related to their membership of the school
- when pupils are participating in online lessons, the same high standard of behaviour is expected. If a lesson is being conducted on a one to one basis, then the pupil should be in a common area of their home and there should be explicit written consent from their parents to authorise it.

Parents/Guardians:

Parents/Guardians play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Ipswich School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/my.ipswich.school and information about national/local online safety campaigns/literature. Parents and guardians will be encouraged to support Ipswich School in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/my.ipswich.school and on-line pupil records
- their children's personal devices in Ipswich School (where this is allowed).

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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

- A planned online safety curriculum should be provided as part of Computing/Life Skills/PSHE lessons and should be regularly revisited. This includes the taking of, and use of images and cyber bullying through online devices.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information

- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement, and encouraged to adopt safe and responsible use both within and outside Ipswich School
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, 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 can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents/Guardians

Many parents and guardians may 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.

Ipswich School will therefore seek to provide information and awareness to parents and guardians through:

- my.ipswich.school
- Parents/Guardians evenings/sessions and ISPost communications

Education & Training – Staff/Volunteers

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand Ipswich School Online Safety Policy and Acceptable Use Agreements
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- The Online Safety Lead will provide advice/guidance/training to individuals as required.

Technical – infrastructure/equipment, filtering and monitoring

Ipswich School will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

Ipswich School technical systems will be managed by the IT Director in ways that ensure that it meets recommended technical requirements:

- There will be regular reviews and audits of the safety and security of Ipswich School technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices
- All users will be provided with a username and secure password by the IT department. Users are responsible for the security of their username and password
- Internet access is filtered for all users
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet
- Ipswich School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

Mobile Technologies including Bring Your Own Device (BYOD)

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

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational.

- The school Acceptable Use Agreements for staff, pupils/students and parents/guardians considers the use of mobile technologies.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/guardians and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer

term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Note: under the General Data Protection Regulations (GDPR) any digital image where a person or persons are clearly identifiable will be classed as 'personal data' and therefore restricted by the GDPR rules – please refer to the School's Compliance Manager and/or the Data Protection/GDPR policy.

Any misuse of digital or video images either inside or outside of school will be dealt with in accordance with the school's behaviour policy.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/guardians (email, social media, chat, blogs, etc) must be professional in tone and content. These communications may only take place on official (monitored) systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class/group email addresses will be provided with individual email addresses for educational use.
- Pupils are taught about online safety issues, such as the risks attached to the sharing of personal details. They are also taught strategies to deal with inappropriate communications and will be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

When using personal social media accounts school staff should ensure that:

- No reference should be made in social media to pupils, parents/guardians or school staff

- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

When official school social media accounts are established there should be:

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

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to proactively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process.

Unsuitable/inappropriate activities

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

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Ipswich School					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	

Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)				X	

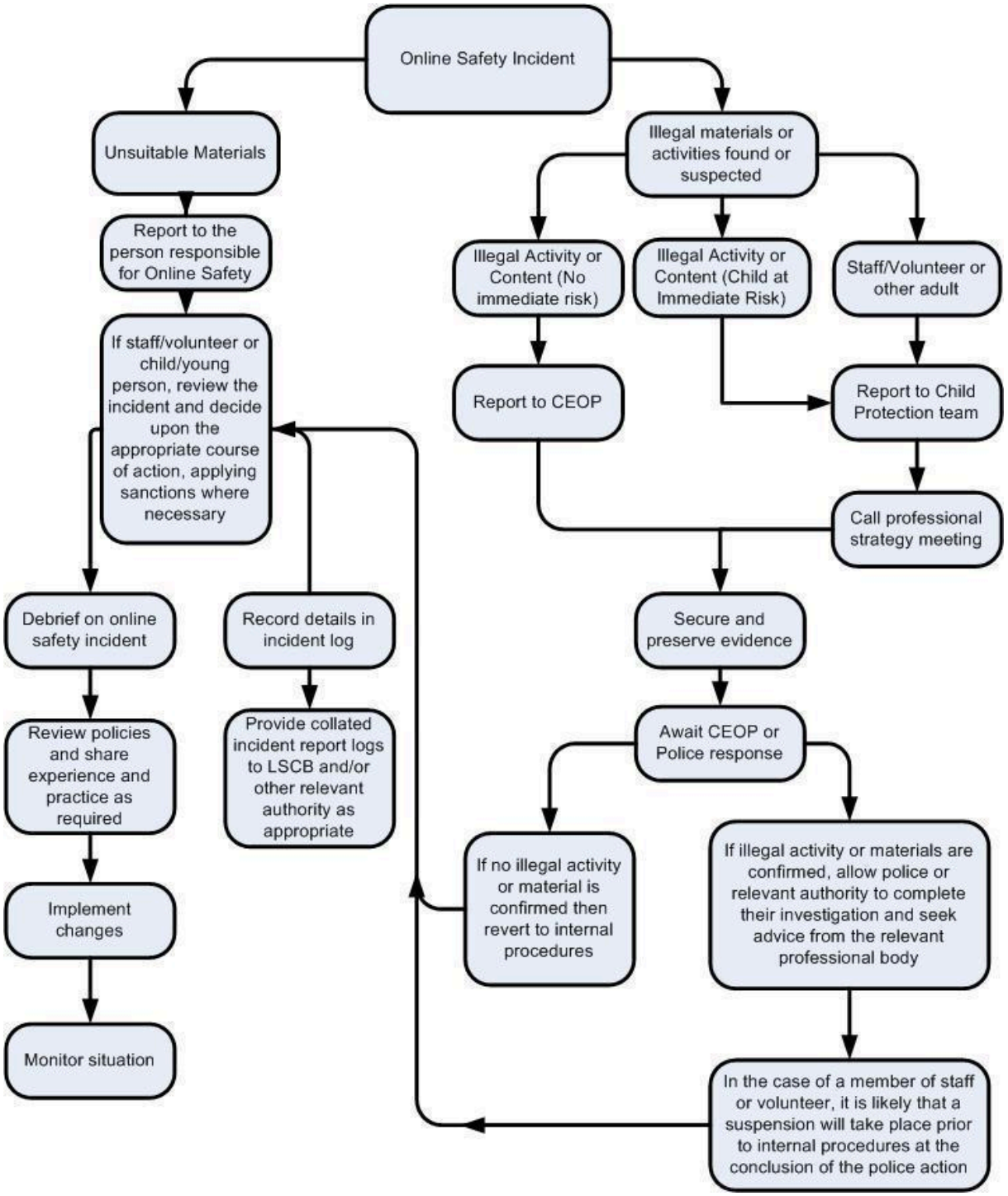
On-line gambling				X	
On-line shopping / commerce				X	
File sharing		X			
Use of social media				X	
Use of messaging apps				X	
Use of video broadcasting e.g. Youtube		X			

Responding to incidents of misuse

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

Illegal Incidents

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



Other Incidents

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

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

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation

Glossary of Terms

AUP / AUA	Acceptable Use Policy / Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of 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
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioner's Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
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
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide 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.

VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

All School policies and HR policies can be found in the Google Shared Drive – School Policies.

Reviewed August 2025