



Gosfield School

Acceptable Use of ICT - Policy for Pupils

Whole School Policy, including EYFS

Table of Contents	Page
Aims and Scope	1
Management of Personal Data & Passwords	2
Unacceptable Use of the School Internet	3
Reporting Concerns and Portable Devices	4
Sanctions for Breaching the Guidelines	5
Responding to Incidents of Misuse Flow Chart	7
Remote Learning	8

AIMS

The purpose of this policy is to ensure that all pupils of Gosfield School understand the ways in which the Information Communication Technology (ICT) equipment is to be used. Our aim is to provide a service within school to promote educational excellence in ICT, innovation, communication and to educate users about online behaviour. This includes interacting with other individuals on social networking websites and in chat rooms and increasing cyber bullying awareness. The policy aims to ensure that ICT facilities and the Internet are used effectively for their intended purpose, without infringing legal requirements or creating unnecessary risk.

ROLES AND RESPONSIBILITIES

The Principal is responsible for approving this policy.

The DSL with the IT Network Manager is responsible for updating this policy and ensuring that it is followed. All staff members of Gosfield School are responsible for applying this policy.

SCOPE

All pupils currently on the attendance register at Gosfield School are set up as users of the school network. This includes pupils from Reception to Year 13. This policy applies to all users of the Gosfield School ICT services and/or infrastructure, and applies when accessing any of the School's systems internally, at home or at an external location.

POLICY STATEMENT

Pupils are provided with free access to a wide range of ICT provision to enable and assist their work and support their educational development. By using the School's provision, all users are automatically agreeing to this policy.

A copy of the policy is included on the website. Before being set up as a user on the school network, all users are expected to read and sign the form at the admissions stage to indicate acceptance of its contents. For the younger pupils in the School - that is those from Reception to Year 6 - their parents are expected to read the policy with them and sign on their behalf. Years 7 to 13 pupils are automatically assumed to accept this policy. If a student chooses to "opt out", then school access will be denied, until confirmation of the acceptance of the rules is received. A further confirmation of the presumed acceptance of this policy appears as a message prior to logging on and users must click ok to accept the terms and conditions. This message appears on any internal school device. By pressing OK confirms the user's agreement.

Users are responsible and personally accountable for their use of the School's ICT systems. Any use that contravenes this policy will be dealt with by the standard disciplinary procedures and may result in them being removed as a user from the school network. This applies to both staff and pupils.

EDUCATION

This Acceptable Use Policy is available to parents and pupils, the School ensures that all pupils are made aware of the policy, and a copy of the policy is available on the School website. Pupils are spending increased amounts of time on devices and mobile phones, as a result they may develop friendships online through gaming and social media platforms which present risks. Pupils are regularly reminded of their responsibility for the use of their device and how to behave appropriately online. Staff are aware that the use of technology can target young people and are expected to be alert to signs of abuse. They must report any concerns they have to the DSL, SLT or the Principal. Preventative action and early help will safeguard our students, both victims and perpetrators will be supported and kept safe if there is evidence that abuse has taken place.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

commerce: - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>).

MANAGEMENT OF PERSONAL DATA

The School operates a number of procedures to protect personal data. These include:

- Secure storage of data
- Secure Storage of pupil personal data
- File encryption when transferring data outside secure networks

MONITORING

The School has an internet filtering system in place designed to remove controversial, offensive or illegal content. However, it is impossible to guarantee that all controversial material is filtered. If you come across any inappropriate website or content whilst using the ICT equipment, you must report it to a member of staff immediately.

The School reserves the right to monitor all activity on the school network and any personally owned device connected to the school network whilst inside the school grounds. All forms of electronic data held on the School's systems are the property of the School. Any member of the Senior Leadership Team can access any data stored on the School's systems at any time to ensure that the system is being used appropriately. At the request of the Principal, or the Head of Prep, the IT Network Manager will investigate if there has been any breach of this policy by searching files and communications on the School's systems. Users should not expect nor assume that their school files, emails and Internet activities are private.

PASSWORDS

All users are allocated a unique username and password. Passwords must always be kept private, should not be written down or given to another user. If a pupil believes that their password has been compromised, they must see the IT Network Manager immediately to have it reset.

UNACCEPTABLE USE OF THE SCHOOL INTERNET

Gosfield School expects all users to use the ICT facilities and the Internet responsibly and strictly according to the following conditions. Users must not use the School's ICT systems:

- For the creation or transmission of obscene, abusive, offensive or indecent images, data or other material, or any data capable of being transformed into obscene or indecent images or material.
- To harass or bully any other person. Any such activity will be treated in the same way as physical bullying and will be subject to the same anti-bullying policy.
- To corrupt or destroying other users' data.
- To violate the privacy of other users.
- To disrupt the work of others.
- To knowingly copy content for research skills and should avoid plagiarism, and uphold copyright regulations
- For the creation of material with the intent to defraud.
- For the creation or transmission of defamatory material.
- For the creation or transmission of content that promotes extremist activity, including terrorism and weapons.
- To post any information on websites or social media that could cause any other member of the School distress, or bring the School into disrepute.
- For private financial gain, or any political or commercial activity.
- To breach the copyright of any materials whilst using the school's ICT systems. This includes, but is not exclusive to:
 - Not copying, or attempting to copy, any of the School's software
 - Not copying the work of another user or engaging in plagiarism
 - Not storing any files in their OneDrive or personal storage area which require copyright permission, and where that permission is not held.
- To download, copy or attempt to install any software onto school computers.
- To deliberately attempt to gain unauthorised access to networked facilities or services, including any attempt to probe, scan or test the vulnerability of the system or network.
- To connect any network-enabled personal device to the school's network without the express permission from the IT Network Manager.
- Use devices to access inappropriate material using 3G/4G/5G networks

Users must not:

- Use another person's account, nor attempt in any way to discover their password. To do so is a clear breach of this policy.
- Bring into school any material that would be considered inappropriate on paper. This includes files stored on CD, DVD or any other electronic storage medium.
- Download, upload or bring into school material that is unsuitable for children or schools. This includes any material of a violent, racist, terrorist or inappropriate sexual nature. The transmission, display, storage or promotion of any such material is a violation of the Computer Misuse Act 1990, and possession of certain types of material can lead to police prosecution.
- Under any circumstances upload staff/student pictures online other than via school owned social media accounts
- Attempt to circumvent the school's firewall and Internet filtering systems. To do so will be treated as a breach of this policy. This includes the use of proxy servers and websites to bypass the Internet filtering system. Such activity will be subject to the standard disciplinary procedures and may result in them being removed as a user from the school network
- Continue to use an item of networking software or hardware after a member of staff has requested that use of it cease because it is causing disruption to the correct functioning of the school's ICT systems.
- Attempt to deny the provision of ICT services to other users by the deliberate or reckless overloading of access links or by switching equipment.
- Introduce a virus or other harmful software to the school's ICT systems.
- Monitor data or traffic on the school's ICT network/systems without the express authorisation of the owner of the network/system.
- Use their personal devices to access inappropriate material. This includes the use of 3G/4G/5G networks.

Any activity carried out under the username of an individual is the responsibility of the named person associated with that username. It is the user's responsibility to ensure that they properly log out of the computer when they have finished using it. Users are responsible for all files that are stored in their storage area and any visits to websites accessed by their user account.

The School encourages all users to use the Internet; however, it is provided for school business and any non-school use of the Internet must be carried out in the user's free time. The School cannot be held responsible for any failed personal financial transaction that may happen whilst using the school's ICT systems.

Any personal ICT equipment physically connected to the school's ICT network must have appropriate, fully functioning and up to date antivirus software protection.

Any breach of copyright whilst using the School's ICT systems is the individual user's responsibility and the School cannot accept any liability or litigation for such a breach.

Any attempt by a user to compromise the security or functionality of the school network and its ICT systems, either internally or externally, will be considered as "hacking". It should be noted that "hacking" is illegal under the Computer Misuse Act 1990 and is prosecutable under law. Any such attempt by a Gosfield School user may result in a referral to the Police and a subsequent Police investigation.

There is a wealth of information on the Internet; however due the open nature of the Internet, a lot of material is either illegal or unacceptable. Any user that thinks inappropriate or illegal material is being accessed must report it to their teacher, line manager or the Network Manager. Any pupil found accessing such material will be subject to sanctions and may result in them being removed as a user from the school network.

The School has robust monitoring and filtering systems in place which will:

- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- identify the device and the unauthorised online platform accessed, alerts are sent to the group pastoral monitoring email including the network manager. The incident is followed up immediately and procedures followed. Where the content raises more serious concerns the safeguarding procedures are followed and any further intervention with outside agencies is implemented.

REPORTING CONCERNS

It is the duty of staff to support the School's safeguarding policy and report any behaviour which is inappropriate or a cause for concern, to a member of staff.

PORTABLE DEVICES

This policy always applies to any portable laptop, tablet, smartphone, smartwatch or other such mobile device used to access Gosfield School systems including email. Devices issued to you by Gosfield School remain the property of Gosfield School and can be recalled for maintenance at any time. Portable devices are provided for business use and any personal use should not be significant. Limited and 'reasonable' personal use is permitted.

The same care with security and confidentiality of information should be taken as would be the case with ICT use within the school. Portable devices must be password protected and should be locked away when not in use. Portable devices should be left out of sight of thieves when in public places and cars. Sensitive or confidential data, and data related to people protected under the Data Protection Act should remain within the security of Office 365 and the School's MIS system.

- Personal devices should be charged before being brought to school as the charging of personal devices is not permitted during the school day
- Devices must be in silent mode on the school site and on school buses
- School devices are provided to support learning. It is expected students will bring devices to-school as required.
- Confiscation and searching (England) - the School has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately
- *Devices may be used in lessons in accordance with teacher direction*

Users should avoid unnecessarily downloading sensitive or confidential information onto portable devices, or storage devices such as USB memory sticks, CDs, DVDs or portable hard drives. Any sensitive or confidential data, as identified through the Data Protection Act 1998, which is for whatever reason downloaded to a portable device or storage device must be encrypted using appropriate encryption software and be password protected.

SANCTIONS FOR BREACHING THESE GUIDELINES

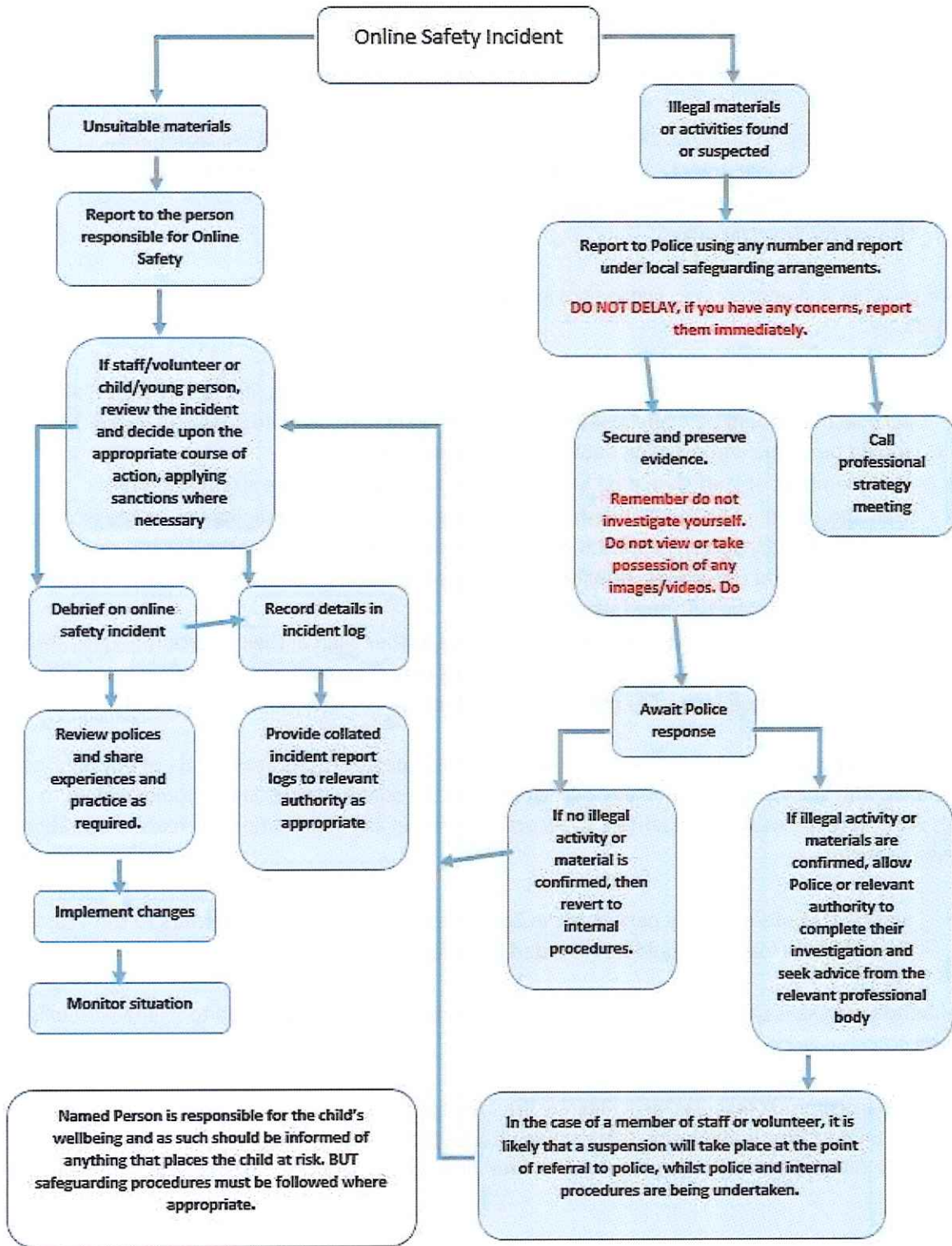
The sanctions imposed on a pupil will vary depending on the severity of the misuse. The sanctions imposed are at the discretion of the Principal and for a pupil may include:

- Removal of internet privileges for 24 hours
- Removal of internet privileges for 7 days
- Permanent withdrawal of Internet privileges
- Detention
- Suspension
- Exclusion

Misuse of the ICT provision or malpractice that compromises the School's network, security or data will have serious consequences. If the incident is identified as a malicious attack, it will be investigated, and any cause for concern identified such as extremism, hate, data breach, gang activity or organised crime will be referred to the relevant authorities and Safeguarding partners. Any action that compromises the School's security may become a Police matter. The Principal will decide when the investigation is complete.

Where there is a concern identified, students should be registered for the Cyber Choices Program. This initiative is aimed at 12-18 year olds supported by the National Crime Agency and the Home Office, together with regional and local police force cyber specialists. The objective of the program is to encourage students to use their cyber skills positively by highlighting alternative opportunities, along with providing victim awareness and deterrents, such as the potential penalties for continuing along the cybercriminal pathway. (When to call the police – Guidance for schools and colleges – NSPCC 2020)

RESPONDING TO INCIDENTS OF MISUSE – FLOW CHART



REMOTE LEARNING

Gosfield School will continue to facilitate remote learning. Working online presents challenges to pupils and both staff and pupils should comply to the code of conduct at all times and have an awareness of the following:

Guidance for staff and pupils is as follows regarding remote learning:

- All participants should ensure backgrounds in videos do not share any personal information or inappropriate content - This should include considerations of whether other members of households are visible or can be heard.
- Appropriate clothing should be worn, and appropriate language should be used by all participants.
- It is advisable to mute/disable learners' videos and microphones in live situations.
- Double check that any other tabs they have open in their browser would be appropriate for a child to see, if they are sharing their screen
- Use professional language

Where possible and appropriate, live events and/or chat messages should be captured and/or recorded.

- Many systems offer the ability for settings to 'record' conferences; if this is the case, all participants should be made aware that the live events are being formally recorded. This should be in line with existing data protection requirements.
- Two members of staff should be present where possible when live streaming events.
- Staff should not provide any one-to-one tutoring, support or messaging unless the activity is pre-approved by leaders. Parental permission should be sought to authorise communication, and in the event of tutoring, another adult known to the child should be present in the home or venue where the tutoring takes place.
- Pupils should be in a shared space in their house, rather than in their bedroom. Pupils should also be appropriately dressed, alternatively staff may request they turn their cameras off, any misconduct will be alerted to parents and students will be sanctioned accordingly.

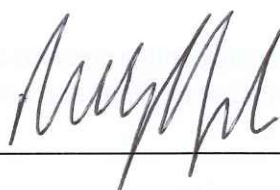
Pupils should be aware of acceptable online behaviour and expectations at the start of any lessons/ live events. This should also include any participation in the chat function. Staff should explain to pupils when it is acceptable for learners to record events and any expectations or restrictions about onward sharing.

- Staff and pupils may only participate in Zoom lessons if there are 3 members to the Team. All Zoom/Teams lessons should be recorded for safeguarding reasons.

If deliberate misuse is brought to the School's attention, it should be responded to in line with existing policies.

Parents/Guardian must take responsibility for the monitoring of safe internet usage when remote learning is taking place in the home setting away from school. This can be done either by placing appropriate filters/parental controls on your home internet connection or by checking your child's device usage.

Signed _____
Principal



Date _____

4/09/2023