FINTON HOUSE
SCHOOL

TECHNOLOGY POLICY
INCLUDING ONLINE SAFETY

Member(s) of staff responsible: Ben Freeman, Catherine Gomez, Andy Dyer

Date Revised: May 2026

A hard copy of this policy is available to all governors and parents on request from the School Office. It is accessible to all staff electronically (in the Policy folder on the Staff Admin Drive) and a hardcopy held on file in the Head's Office. This policy applies to all at the School including those in Reception (the EYFS).

Contents

Version	Policy Update
May 2026	Added clause regarding Mobile phone use by pupils in Section 10

1. Policy Statement

This policy applies to all members of the School community (including governors, staff, pupils, volunteers, parents and visitors) who have access to and are users of the Finton House IT systems, both in and out of the School. The policy should be read in conjunction with the Child Protection and Safeguarding policy.

The Education and Inspections Act 2006 empowers Headteachers 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 cyberbullying 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 Pastoral Care Policy.

The School will actively promote responsible use of all IT systems by all users (pupils and adults), both when on site or when use of IT is connected in some way to membership of the School community.

2. The Governing Body

Responsibilities

The Governors ensure there are appropriate filters and monitoring systems in place and they are careful that 'over blocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding. They are responsible for the approval of the Technology Policy (including Online Safety) policy and for reviewing the effectiveness of the policy. The annual review of this policy will be carried out by the Technology Working Group and approved and monitored by the Pastoral Committee. Regular information about online safety incidents and monitoring reports are shared with governors at the termly Safeguarding Committee meeting. The Technology Working Group is made up of:

- The Head
- Deputy Head Academic
- Deputy Head Pastoral/DSL
- Assistant Head: Technology
- Head of Information Systems

with consultation from the Chair of Governors, Safeguarding Governor and IT Governor.

The group will termly review online safety and make action-based decisions as required.

Responsibilities

- Ensuring all actions and decisions are aligned to the School's policies, including the IT vision and strategy, the Child Protection and Safeguarding Policy and the Acceptable Use Agreement.
- Ensuring any decisions, including financial, support robust online safety and the teaching and learning at the School, and the business processes.
- Ensuring any decisions impacting users are clearly communicated and understood.
- Consulting stakeholders, including parents and the pupils about the online safety provision.

Another member of the Governing Body has the role of Child Protection & Safeguarding Governor which includes Online Safety. The role will include:

- Meetings with the DSL.
- Feedback about online safety.
- Monitoring of network, internet, filtering and incident logs.
- Reporting to the Board of Governors.
- The review and monitoring of the School Online Safety policy and documents.

- Mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression.

Training

Governors should take part in online safety training and awareness sessions, with particular importance for those who are members of any subcommittee or group involved in technology, online safety, health & safety and safeguarding. This may be offered in a number of ways:

- Attendance at training provided by a relevant organisation.
- Participation in school training or information sessions for staff or parents.

3. The Head and Senior Leaders

Responsibilities

The Head has a duty of care for ensuring the safety (including online safety) of members of the School community, although the day to day responsibility for online safety will be delegated to the DSL.

The Head and DSL should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff, (see flow chart “Incidents of misuse” and Schools Actions and Procedures).

The DSL and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Head and Deputy Head Pastoral/DSL will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

4. The Designated Safeguarding Lead (DSL)

Responsibilities

The DSL takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the School online safety policies and documents. This includes:

- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Providing training and advice for staff.
- Liaising with school technical staff.
- Receiving reports of online safety incidents and creating a log of incidents to inform future online safety developments.
- Meeting with the Child Protection & Safeguarding Governor to discuss current issues, review incident logs, filtering logs and change control logs.
- Attending Technology Working Group meetings.
- Attending Safeguarding Committee meetings.
- Reporting about online matters to the Senior Leadership Team.

The DSL should be trained in Online Safety issues and be aware of the potential for serious child protection & safeguarding issues to arise from:

- Sharing of personal data.
- Access to illegal / inappropriate materials (including use of social media).
- Inappropriate on-line contact with adults / strangers.
- Potential or actual incidents of grooming.
- Cyberbullying.

- Radicalisation
- Exposure to misinformation, disinformation and online conspiracy theories

5. The Head of Information Systems

Responsibilities

The Head of Information Systems is responsible for ensuring that:

- The School's technical infrastructure is secure and is not open to misuse or malicious attack.
- The School meets required online safety technical requirements.
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed, with the use of multi-factor authentication where appropriate.
- The filtering of the network is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person as Smoothwall support this process (see "19. Technical Security" for good practice.
- They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- The use of the network, internet, Frog VL, School Manager, remote access and email is regularly monitored in order that any misuse/attempted misuse can be reported to the Head or DSL for investigation, action and sanction if appropriate.
- Monitoring software / systems are implemented and updated as agreed in school policies.

School technical systems will be managed in ways that ensure that the School meets recommended technical requirements:

- There will be regular reviews and audits of the safety and security of the School's 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 (pupils and adults) will be provided with a username and password by the IT service provider who will keep an up-to-date record of users and their usernames. Reception and Year 1 will use the same simple password. Year 2 to Year 6 are given a unique username and password to be used throughout their time at Finton House School. Staff change their password twice a year in September and April.

- The passwords for the School's IT system, used by the IT service provider, must also be available to the Head and should be kept in the School safe.

- The IT service provider is responsible for ensuring that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations.

- Internet access is filtered for all users. Illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored (Smoothwall). Requests for filtering changes must be made to the IT Team and subsequently approved by the Head, Deputy Head Academic or DSL.

- Internet filtering should ensure that pupils are safe from terrorist and extremist material including radicalisation when accessing the internet.

- The School has provided enhanced and differentiated user-level filtering through Smoothwall filter and firewall; (allowing different filtering levels for different ages and different groups of users – staff / pupils / visitors, etc.).

- The IT Service provider regularly monitors and records the activity of users on the School technical systems and users are made aware of this in the Acceptable Use Agreement;

- An appropriate process is in place for users to report any actual / potential technical incident or security breach to the IT team.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, 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 anti-virus software.

- An agreed policy is in place for the provision of temporary access of "guests" (e.g.: trainee teachers, supply teachers, visitors) onto the School systems.

- An agreed policy is in place regarding the extent of personal use that users (staff and pupils) and their family members are allowed on school devices that may be used out of school (see AUA).

- An agreed policy (AUA) is in place surrounding the downloading of executable files and installing programmes on school devices.

- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the School site unless safely encrypted or otherwise secured, (see Data Protection Policy).

6. **The Staff of Finton House**

Responsibilities

All staff are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school Technology Policy including Online Safety policy and practices.
- They know how to report any child-on-child abuse or other safeguarding concerns (see Child Protection and Safeguarding policy) to the DSL immediately.
- They have read, understood, and signed the Staff Acceptable Use Agreement, which includes remote learning/video conferencing. They are aware of expected staff behaviour outlined in the Employment Handbook.
- They report any suspected misuse or problem to the Head or DSL for investigation.
- All digital communications with pupils, parents or carers should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- They monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies regarding these devices.
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that any unsuitable material that is found in internet searches is reported immediately via CPOMS.

Training

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:

- Staff complete the Educare module on Online Safety, and other related IT safety training such as Boxphish, The Key etc. This will be regularly reinforced.
- All new staff receive online safety training as part of their induction program, ensuring that they fully understand the School Technology Policy including Online Safety policy and Acceptable Use Agreements.

- It is expected that some staff will identify online safety as a training need within the appraisal process.
- The DSL will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Technology Policy including Online Safety policy and its updates will be presented to and discussed by staff.
- The DSL will provide advice / guidance / training to individuals as required with the support of the IT Team and Assistant Head: Technology.

7. The Pupils

Responsibilities

As pupils move through the School, they need to become increasingly aware of the need to take responsibility for their own actions and use of IT systems and hardware. This includes:

- Being responsible for using the School's digital technology systems in accordance with the Acceptable Use Agreement, which includes being online at home/remote learning.
- Understanding the importance of reporting abuse, misuse or access to inappropriate materials and knowing how to do so.
- Understanding the importance of adopting good online safety practice when using digital technologies out of school.
- Having a steadily increasing understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Acceptable Use Agreement

From Year Three to Six, the Computing Teacher reads through the AUA with the children and they sign two copies; one is kept at school and the other copy is sent home for parents. From Reception to Year Two, the Computing Teacher reads through the AUA with all children.

AUAs are displayed on the walls of every classroom in school as a visual reminder to pupils.

Pupils in Years Five and Six sign two copies of an additional 1:1 iPads AUA; one is kept at school and the other copy is sent home for parents.

Education

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. Pupils need the help and support of the School to recognise and avoid online safety risks and build their resilience to this aspect of their lives. Children can report any online safety concerns or cyberbullying worries to any member of staff but can also use the Frog Pastoral page and alerts are then sent to staff who respond during the School week.

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

- A planned online safety curriculum is provided as part of Computing, PHSEE/RSE and other lessons and should be regularly revisited.
- Key online safety messages are reinforced as part of a planned programme of assemblies and pastoral activities. This also includes year group workshops and external provision e.g. Childnet.
- The pupils are taught in all subjects to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- The pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

- The pupils are 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.
- The pupils are helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff act as good role models in their use of digital technologies, the internet and mobile devices
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites pupils visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs or discrimination) that would normally result in internet searches being blocked. In such a situation, staff should notify the IT Team/Assistant Head: Technology.

Scratch

Scratch is a high-level block-based visual programming language and website aimed primarily at children as an educational tool for programming. It was developed by the MIT Media Lab and is used to teach coding by schools world-wide. Pupils in Years Three to Six are assigned accounts by the Assistant Head: Technology to enable them to use this online platform.

School Responsibilities

- Pupils are given a unique username and password by the Assistant Head: Technology. They are encouraged not to share this information per the school's Acceptable Use Agreement.
- Usernames do not include any personal information about pupils.
- The Assistant Head: Technology uses an educator account which enables them to assign pupils into 'Classes' and review content pupils are creating.
- The educator account is assigned to a specific email address which can be monitored by the Assistant Head: Technology and IT Technician. This email address will remain active on the school system should either role be filled by a new staff member.
- The Assistant Head: Technology will regularly check pupil account activity on the Scratch platform
- Where available, commenting is turned off.
- Staff and pupils will report any content which is not appropriate to the Scratch administrators.
- Scratch Privacy and Security Commitments:
  Scratch is in compliance with all United States federal laws that are applicable to MIT and the Scratch Foundation, the organizations that have created and maintained Scratch.
  The Scratch Team reviews reported comments and projects every day and has policies in place to deal with any which may violate its community guidelines.
  Scratch uses basic demographic data (in aggregated form) in research studies however does not use specific personal information.

8. **The Parents**

For the purposes of this policy, 'Parents' also includes any carers responsible for pupils at Finton House.

Responsibilities

Parents play a crucial role in ensuring that their pupils understand the need to use the internet and mobile devices in an appropriate way. The School will take every opportunity to help parents understand these issues through parents' workshops, newsletters, the School's VLE (Frog Learn) including information about national and local online safety campaigns or literature. Parents and carers will be encouraged to support the School in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Access to parents' sections of the website, Frog VLE and on-line pupil records.
- Their pupils' personal devices in the School (where this is allowed).

- Video-conferencing use for home use or remote learning.

Education

Some parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their pupils and in the monitoring / regulation of the pupils' on-line behaviours. Parents may underestimate how often pupils come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The School will therefore seek to provide information and awareness to parents and carers through:

- High profile events and campaigns e.g.: Safer Internet Day.
- Reference to the relevant websites, publications e.g.:
  SWGfl - swgfl.org.uk
  Internet Matters.org - https://www.internetmatters.org
  Thinkuknow - https://www.thinkuknow.co.uk/
  Net Aware - https://www.net-aware.org.uk/
  UK Safer Internet Centre - https://www.saferinternet.org.uk/
  Parent Info – https://parentinfo.org/
  London Grid for Learning - https://www.lgfl.net/online-safety/default.aspx
  CEOP - https://www.ceop.police.uk/safety-centre/
  Childline - https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/
  0800 1111 who are operating a 9am – Midnight service in response to COVID-19.
  NSPCC - https://www.nspcc.org.uk/keeping-children-safe/online-safety/
  Childnet - https://www.childnet.com/parents-and-carers/parent-and-carer-toolkit
  Let's Talk about It - https://www.ltai.info/staying-safe-online/

9. Overview of Responsibilities

No	Area		Sub Area	Owner
1	IT Strategy	1.1	Generate / update	Assistant Head: Technology
		1.2	IT communication	Head of Information Systems
		1.3	Define user requirements	Head of Information Systems
		1.4	Review system requirements v. strategy	Assistant Head: Technology Head of Information Systems
2	Budgets, purchasing & Contracts	2.1	Running costs budget	Head of Information Systems
		2.2	IT Cap-Ex budget	Director of Finance & Operations
		2.3	Budget recommendations	Assistant Head Technology Head of Information Systems
		2.4	Approve purchases	Director of Finance & Operations
		2.5	Purchase IT resources	Head of Information Systems
		2.6	3rd Party contracts, KPIs	Director of Finance & Operations
3	Documentation, procedures, policies & processes	3.1	Systems and services documents	Head of Information Systems
		3.2	Technology & Online Safety policy	Head/DSL

No	Area		Sub Area	Owner
		3.3	Define policies, processes and procedures	Director of Finance & Operations
		3.4	Password security	DFO/Head Head of Information Systems
4	Reporting	**4.1**	IT services & systems	Head of Information Systems
		4.2	Progress of works/projects	Head of Information Systems
			Satisfaction surveys	Director of Finance & Operations
5	Server Environment	**5.1**	New School Servers	Elmbrook
		5.2	Old Servers	Elmbrook
		5.3	Domain Management	Director of Finance & Operations
6	Class Room Environment	**6.1**	Boards / Panels	Head of Information Systems
		6.2	Mobiles for trips	Head of Information Systems
		6.3	Desktops/ iPads / laptops	Head of Information Systems
		6.4	Printers	Head of Information Systems
7	Management Information System	**7.1**	Software	Head of Information Systems
		7.2	Data	School Administrator
8	Operating Software	**8.1**	Windows	Elmbrook
		8.2	VLE	Deputy Head: Academic
		8.3	Dashboard	Elmbrook
		8.4	Anti Virus	Elmbrook
		8.5	Print management	Head of Information Systems / Bursar
		8.6	Jamf	Head of Information Systems
9	iPads	**9.1**	Apps	Head of Information Systems
10	PCs and Laptops	**10.1**	Hardware	Head of Information Systems
11	Data Management	**11.1**	Back up	Elmbrook
		11.2	GDPR compliance	Director of Finance & Operations Head of Information Systems
12	Helpdesk	**12.1**	Licenses	Head of Information Systems
		12.2	Open items	Director of Finance & Operations
13	Safeguarding	**13.1**	Smoothwall	Head of Information Systems DSL

No	Area		Sub Area	Owner
		13.2	Monitoring	DSL, Head of Information Systems and Safeguarding Lead Governor
		13.3	Email addresses	Head of Information Systems Assistant Head Technology / DSL
14	Training programme	**14.1**	New joiners	Head of Information Systems
		14.2	Inset day	Head of Information Systems
		14.3	Frog/VLE	Deputy Head: Academic
		14.4	Parents/Students home support	Head of Information Systems
		14.5	Online safety	Assistant Head: Technology
15	Social Media/ Digital	**15.1**	All channels (FB, X, Linkedin, website)	Head of Marketing, Communications and Development
16	Safety and insurance	**16.1**	PAT testing	Director of Finance & Operations
		16.2	Cable safety review	Head of Information Systems
		16.3	Insurance cover	Director of Finance & Operations
		16.4	All items security marked and on asset register	Head of Information Systems

10. Mobile Technologies

Mobile technology devices may be school owned 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 which may include Engage, Frog VLE and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the devices in a school context is educational. The AUA covers mobile technologies and is consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Pastoral Care Policy and Anti-Bullying Policy and Acceptable Use Agreement. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the School's Online Safety education programme.

The School allows the following devices:

	School Devices		**Personal Devices**		
	School owned for single user (staff)	School owned for multiple users (pupils)	Pupil owned	Staff owned	Guest owned
Allowed in school	*Yes*	*Yes*	*Y6 only (kept in Reception)*	*Yes*	*Yes*

Full network access	*Yes*	*Yes*	*No*	*Yes*	*No*
Internet only	*n/a*	*n/a*	*No*	*n/a*	*Yes*
Remote server	*Yes*	*No*	*No*	*Yes*	*No*

School mobile devices are allocated as follows:

iPads

All teachers are provided with an iPad. There are also 60 located outside the library which can be booked out by a member of staff for pupil use and maybe booked out by a teaching assistant for their own use. There are 90 iPads allocated for individual use by pupils in Year Five and Six.

Laptops

All teachers and admin staff have been allocated a laptop. There are also 32 located outside the library and an additional 32 located on the second floor which can be booked out by a member of staff for pupil use.

The School manages all the devices, including the installation of apps and software, the changing of settings and monitoring of use.

All school iPads are controlled though the use of Mobile Device Management software, JAMF.

Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g.: Internet only access, network access allowed, shared folder network access).

For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted. The filtering of all devices accessing the School systems is through Smoothwall and is set per user. Where the user cannot be determined (i.e.: due to a group log-in being used) the access will be very restricted.

Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user. These may include; revoking links between software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licenced software etc.

All school devices are subject to proactive routine monitoring.

Staff iPads may be taken off site, but should never be left unattended, nor the passcode shared or removed. They should not be used by anyone else, including family members. Pupil iPads and laptops may only be taken off-site within the local area for teaching and learning purposes.

Individual iPads for Year Five and Six pupils may be taken off site once pupils have signed the AUA and parents have acknowledged agreement to the Home-School Agreement by Finton Post.

Personal use of school devices is permitted, but within the terms of the AUA and so long as it does not interfere with or compromise professional duties or responsibilities. See Use of Mobile Devices in EYFS Policy.

All users of school devices are entitled to technical support from the IT Team.

The changing of settings (exceptions include personal settings such as font size, brightness, etc.) that would stop the device working as it was originally set up and intended to work is not permitted.

The software / apps originally installed by the School must remain on the School owned device in usable condition and always be easily accessible. From time to time the School may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps.

The School will ensure that school devices contain the necessary apps for schoolwork. Apps added by the School will remain the property of the School and will not be accessible to students on authorised devices once they leave the School roll. Any apps bought by the user on their own account will remain theirs.

Children are not allowed to use mobile phones in school. However, the school recognises that they are a useful tool in life and especially when walking to and from school unaccompanied. Year 6 children who do so are allowed, upon school's receipt of a completed parental consent form, to bring a non-smart phone to school as long as it is switched off and handed into the Office at the beginning of the day and collected at the end of the day.

Personal Mobile Devices

All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access.

Staff are also advised that personal devices including mobile phones, cameras, home laptops, iPads or any mobile technology should not be used to download or store school data including files, folders, images or emails. They should never contain photographs of pupils or be used to contact pupils.

Personal devices are brought into the School entirely at the risk of the owner and the decision to bring the device into the School lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school.

The School accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the School (the School recommends insurance is purchased to cover that device whilst out of the home).

The School accepts no responsibility for any malfunction of a device due to changes made to the device while on the School network or whilst resolving any connectivity issues.

The School recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the School. Pass-codes or PINs should be set on personal devices to aid security.

The School is not responsible for the day-to-day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.

Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition;

- Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements. See Safeguarding Policy.
- Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on viruses or malware to the network.
- Users are responsible for charging their own devices and for protecting and looking after their devices while in school.
- Devices must be in silent mode on the School site and on school minibuses.
- School devices are provided to support learning.
- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- 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.

- Staff owned devices should not be used for personal purposes during teaching sessions or when on duty, unless in exceptional circumstances.
- Printing from personal devices will not be possible.

11. Insurance

School devices are covered by the School's contents insurance policy. Incidents of loss, theft or damage to a school mobile device should be reported to the Director of Finance & Operations who will decide whether to make an insurance claim. If no responsibility can be proved for the damage or loss of the device then the School will arrange repair or replacement.

The School has implemented an "authorised device" approach. Users who have been allocated a device for work use sign an agreement assuming responsibility for that device. The user is liable to replace the item if their behaviour is deemed to have been negligent.

12. 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 and pupils need to be aware of the risks associated with publishing digital images on the internet, potentially creating a digital footprint. 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:

1. When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g.: on social networking sites.
2. Written permission from parents or carers will be obtained via a consent form to agree / not agree to photographs of their child being published on the School website, social media and local press.
3. In accordance with guidance from the Information Commissioner's Office, parents are welcome to take videos and digital images of their pupils at school events (except swim galas) 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 or made publicly available on social networking sites, nor should parents comment on any activities involving other pupils in the digital / video images.
4. Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
5. If parents have expressed a preference for the School to avoid taking or publishing images of their child/children in certain circumstances, they should follow this.
6. Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute.
7. Pupils must not take, use, share, publish or distribute images of others without their permission.
8. Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
9. Pupils' full names will not be used anywhere on a website or blog in the public domain, particularly in association with photographs.

13. **Video-Conferencing and Offsite Teaching in Extreme Circumstances**

All staff who interact with children remotely online will continue to look out for signs a child may be at risk. Any concerns will be followed up on, as detailed in the Child Protection & Safeguarding policy. Staff and pupils' AUA's cover remote learning. On Frog (VLE) there is a digital safety portal for parents to access information and where they can report a concern.

Video-conferencing of pupils is conducted using Teams and access codes to the lessons are embedded within password protected Frog (VLE), so never in the public domain. There is an encrypted password in the link, so even if someone guessed the access code, it still would not work. Before joining, the meeting there is a waiting room so no participant can join unless the host accepts him or her into the meeting from here. As there are small numbers within any meeting it is easy for the member of staff to see whom they are inviting in.

14. **Communications**

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows permissions for various devices and actions in school:

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be used in school	☐							☐
Use of mobile phones in lessons				☐				☐
Use of mobile phones in social time	☐							☐
Taking photos on private mobile phones / cameras				☐				☐
Use of other private mobile devices e.g.: tablets		☐						☐
Use of personal email addresses in school, or on the School network		☐						☐
Use of school email for personal emails				☐				☐
Use of private messaging apps in school, or on the School network		☐						☐
Use of social media in school, or on the School network		☐						☐
Use of external blogs in school, or on the School network		☐						☐

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the School email service to communicate with others when in school, or on school systems (e.g.: by remote access).

  Users must immediately report to the DSL 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 (email, social media, chat, blogs, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the School website and only official email addresses should be used to identify members of staff.

- All staff will ensure good practice when sending email, taking extra care to ensure that emails are sent to the right recipient(s).

- All school data is disclosable under a subject access request and therefore staff should always be aware that anything written in an email could be disclosed to anyone the information is related to, even if it is not addressed to them.

15. **Social Media**

Finton House has a duty of care to provide a safe learning and working environment for pupils and staff and users are also bound by the terms of the Acceptable Use Agreements with regard to social media.

Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the School liable to the injured party. The School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the School through:

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

All school staff should ensure that:

- No reference is made in social media to pupils, parents 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.

- WhatsApp and other similar group chat sites should not be used to communicate with parents, and if a member of staff is part of a group because their child is in that class or year group, any engagement must represent the views of the School.

The School's Social Media Accounts

The management of the School's social media includes:

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

Personal Use of Social Media

Personal communications are those made via personal social media accounts. In all cases, where a personal account is used there must be no reference to or association with the School or incur any impact on the School and its reputation. Personal communications which do not refer to or impact upon the School are outside the scope of this policy.

The School permits reasonable and appropriate access to private social media sites. However, where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Monitoring of Public Social Media

As part of our active social media engagement, the Head of Marketing, Communications and Development pro-actively monitors the internet for public postings about the School, reporting any concerns to the Head. If you become aware of any defamatory comments about the School, you should inform the Head.

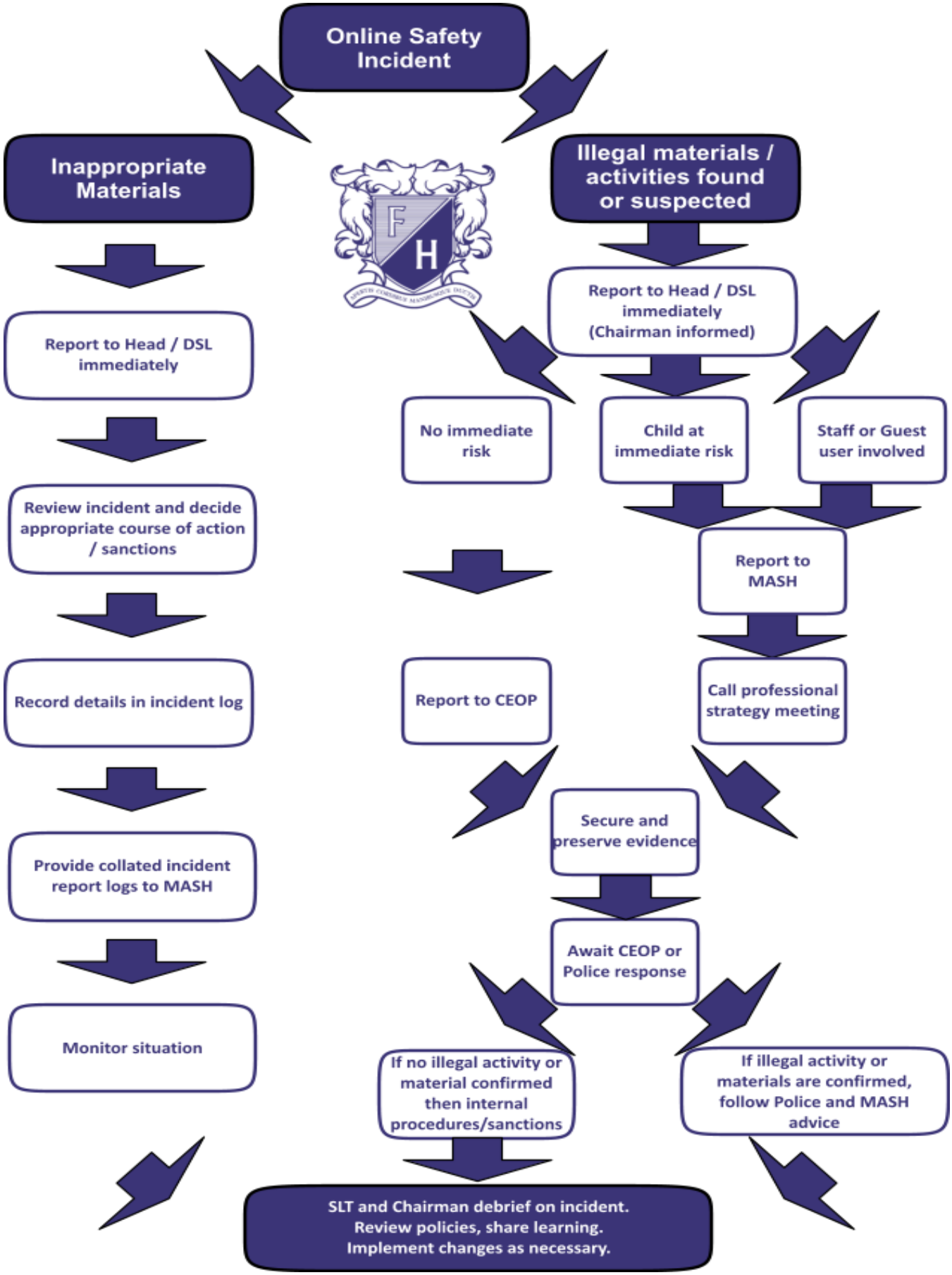
16. Unsuitable/Inappropriate Activities

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

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

User Actions		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 pupils. Contrary to The Protection of Pupils Act 1978					□
	Grooming, incitement, arrangement or facilitation of sexual acts against pupils Contrary to the Sexual Offences Act 2003.					□
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) contrary to the Criminal Justice and Immigration Act 2008					□
	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					□
	Pornography				□	
	Promotion of any kind of discrimination				□	
	Threatening behaviour, including promotion of physical violence or mental harm				□	
	Promotion of extremism or terrorism				□	
	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				□	
Using school systems to run a private business					□	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the School					□	
Infringing copyright					□	
Revealing or publicising confidential or proprietary information (e.g.: financial / personal information, databases, computer / network access codes and passwords)					□	

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Creating or propagating computer viruses or other harmful files				□	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				□	
On-line gaming (educational)		□			
On-line gaming (non-educational)				□	
On-line gambling				□	
On-line shopping / commerce		□			
File sharing	□				
Use of social media		□			
Use of messaging apps		□			
Use of video broadcasting e.g.: Youtube			□		


Online Safety Incident
Inappropriate Materials
Illegal materials / activities found or suspected
Report to Head / DSL immediately
Report to Head / DSL immediately (Chairman informed)
No immediate risk
Child at immediate risk
Staff or Guest user involved
Review incident and decide appropriate course of action / sanctions
Report to MASH
Record details in incident log
Report to CEOP
Call professional strategy meeting
Secure and preserve evidence
Provide collated incident report logs to MASH
Await CEOP or Police response
Monitor situation
If no illegal activity or material confirmed then internal procedures/sanctions
If illegal activity or materials are confirmed, follow Police and MASH advice
SLT and Chairman debrief on incident.
Review policies, share learning.
Implement changes as necessary.

17. 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. Alerts are usually triggered by the School's filtering system, 'Smoothwall'. All 'danger' alerts are investigated within 48 hours by the DSL with the support of the IT Team.

Illegal Incidents

If there is any suspicion that a website has been accessed at school which 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 school policy. However, there may be times when infringements of the policy could take place, through careless, irresponsible or, very rarely, deliberate misuse. Misuse which goes against the AUA and Finton Code of Code will be recorded as a Low-Level Concern on Confide.

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer (usually the Head's or /DSL's) 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 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). Both the Head and DSL have a VNL link on their computers to check URL addresses, and the link is monitored.

- 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 unless these are images, in which case this is not permitted.

- 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.
    - Referral to MASH and/or the LADO if it involves staff.
    - 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.

- It is important that all of the above steps are taken as they will provide an evidence trail for the School and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes.

School Actions and Sanctions

- It is more likely that the School will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the School community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

REPORTING LOG - monitoring and filtering (Smoothwall)

Name	Date	Time	Alert level	Category	URL	Outcome	Shared with who?	Safeguarding file?	Open/Closed?

18.School Actions and Sanctions

Pupil Incidents	Refer to class Teacher	Refer to HeadHeadteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	□	□	□	□	□	□		□
Unauthorised use of non-educational sites in school	□			□	□		□	
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	□	□			□		□	
Unauthorised / inappropriate use of social media / messaging apps / personal email	□	□		□	□		□	
Unauthorised downloading or uploading of files	□			□			□	
Allowing others from outside school to access school network by sharing username and passwords	□	□		□	□	□	□	
Attempting to access or accessing the School network, using another student's / pupil's account	□	□		□	□		□	
Attempting to access or accessing the School network, using the account of a member of staff	□	□		□	□		□	□
Corrupting or destroying the data of other users	□	□		□	□		□	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	□	□		□	□		□	□
Continued infringements of the above, following previous warnings or sanctions	□	□		□	□	□		□
Actions which could bring the School into disrepute or breach the integrity of the ethos of the School	□	□			□	□	□	□
Using proxy sites or other means to subvert the School's filtering system	□	□		□	□		□	□
Accidentally accessing offensive or pornographic material and failing to report the incident	□	□		□	□		□	
Deliberately accessing or trying to access offensive or pornographic material	□	□		□	□	□		□
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	□	□		□	□		□	

Staff Incidents	Refer to DSL	Refer to Head	Refer to Governors	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Dismissal
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	□	□	□	□	□		□
Using personal devices to record images of pupils e.g. to take photographs.	□	□				□	
Inappropriate personal use of the internet / social media / personal email	□	□				□	
Unauthorised downloading or uploading of files		□				□	
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the School network, using another person's account		□			□	□	
Careless use of personal data e.g.: holding or transferring data in an insecure manner		□			□		
Deliberate actions to breach data protection or network security rules		□			□	□	
Deliberately corrupting or destroying the data of other users or deliberate damage to hardware or software		□	□	□	□		□
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	□	□				□	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	□	□				□	
Actions which could compromise the staff member's professional standing		□	□			□	
Actions which could bring the School into disrepute or breach the integrity of the ethos of the School		□	□			□	□
Using proxy sites or other means to subvert the School's filtering system		□			□	□	□
Accidentally accessing offensive or pornographic material and failing to report the incident	□	□			□	□	
Deliberately accessing or trying to access offensive or pornographic material	□	□	□		□	□	□
Breaching copyright or licensing regulations		□				□	
Continued infringements of the above, following previous warnings or sanctions						□	□

19.Technical Security Including Filtering and Passwords

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The School will ensure that the IT infrastructure is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access.
- No user should be able to access another's files (other than that allowed for monitoring purposes within the School's policies).
- Access to personal data is securely controlled in line with the School's personal data policy.
- Logs are maintained of access by users and of their actions while users of the system.
- There is effective guidance and training for users.
- There are regular reviews and audits of the safety and security of school computer systems.
- There is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of the IT Team.

Technical Security

- School technical systems will be managed in ways that ensure that the School meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- Appropriate security measures are in place to protect the following from accidental or malicious attempts which might threaten the security of the School systems and data:
    - Servers: locked server room with air conditioning and racking with adequate ventilation.
    - Firewalls: Supplied by Smoothwall and compliant with KCSIE.
    - Switches: Housed in appropriate locked cabinets out of reach.
    - Wireless system: Password protected and clear policies in place regarding 'Guest' users.
    - Workstations: All security marked and logged in the asset register.
    - Mobile devices: Security marked and logged in asset register. All staff who have been provided with an iPad have signed an agreement for use and security. Responsibilities for the management of technical security are assigned to the IT Team.
- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the IT Technician and will be reviewed, at least annually, by the Online Safety Committee
- Users will be made responsible for the security of their username and password and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security (See Password section below)
- The IT Team is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations. (Inadequate licencing could cause the School to breach the Copyright Act which could result in fines or unexpected licensing costs).
- Mobile device security and management procedures are in place with each device numbered and a booking system used. Each device is also security tagged and locked away at night.

- The Head, DSL and Safeguarding Governor 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.
- An appropriate process is in place for users to report any actual / potential technical incident to the IT Team and administrators (including the Head, Deputy Head Academic and DSL).
- There is an Acceptable Use Agreement in place for temporary access of "Guest" users (e.g.: trainee teachers, supply teachers, visitors) onto the School system, which is time limited as appropriate.
- Staff may use school devices for personal use at school and at home, but only in accordance with the Acceptable Use Agreement and as long as this does not impinge on school responsibilities and duties. Particular care needs to be taken to ensure personal images, etc. are not stored on school devices or the network.
- The School infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc. Users all sign an agreement that they will not try and bypass this protection.
- Personal data cannot be sent over the internet or taken off the School site unless safely encrypted or otherwise secured.

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

- All school networks and systems are protected by secure passwords that are regularly changed, with multi-factor authentication in place as appropriate.
- Any staff member that wishes to use their own device with the Finton Wi-Fi has to login via the BYOD (Bring Your Own Device) wireless network. This is to ensure that we have accountability and security on the Finton network,
- Any visitor wishing to use the Finton Wi-Fi is given login details and a password from the School Office. It is changed regularly. If there is a concern about accountability and security on the Finton network we are able to identify, which visitor it may have been via the electronic sign in and out system.
- The "master administrator" passwords for the School systems, used by the technical staff are available to the Head and Director of Finance & Operations and will be kept in a secure place.
- Passwords for new users, and replacement passwords for existing users will be allocated by the IT Team, forcing the user to create a new password on first log-on.
- Users will change their passwords at regular intervals – as described in the staff and student / pupil sections below.

Staff Passwords

All staff users will be provided with a username and default password by the IT Team who will keep an up to date record of users and their usernames. At first log-on after the account is set up or the password is reset, the user will be forced to provide a new password. The password must:

- Be a minimum of 12 characters long and a maximum of 16.
- Include uppercase and lowercase characters, numbers, symbols (although some services do not allow symbols in passwords).
- Not include proper names or any other words that are related to the account in question e.g. your name, company name, business name, mother's maiden name, address, or anything that may also be used for the security questions.
- Be different for different accounts, to ensure that other systems are not put at risk if one is compromised, and should be different for systems used inside and outside of school.

Password administration

- The account will automatically be “locked out” following six successive incorrect log-on attempts.
- Passwords shall not be displayed on screen, and shall be securely hashed (by use of one-way encryption).
- Staff passwords are monitored by the IT Team. It will not be possible to re-use a password for 6 months and a new one should be significantly different from previous passwords created by the same user. The last four passwords cannot be re-used.

Pupil’s Passwords

- All users (except pupils in Reception and Year 1) will be provided with a username and password by the IT Team who will keep an up to date record of users and their usernames.
- Pupils will be taught the importance of password security.
- The complexity of passwords is set with regards to the cognitive ability of the pupils:
    - Reception and Year 1: Class log-on (used by pupils only).
    - Year 2 – 6: unique password of at least 6 letters (including at least 2 capitals) and 2 numbers.

Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users, even if class log-ins are being used.

Members of staff will be made aware of the School’s password policy:

- At induction.
- Through the School’s Online Safety policy and password security policy.
- Through the Acceptable Use Agreement.

Pupils will be made aware of the School’s password policy:

- In Computing lessons. Through the Acceptable Use Agreement.

Audit / Monitoring / Reporting / Review

The IT Technician will ensure that full records (manual or automated) are kept of:

- User Ids and requests for password changes.
- User log-ins.
- Security incidents related to this policy.

Filtering: Responsibilities

The responsibility for the management of the School’s filtering policy will be held by the Online Safety Committee. They will manage the School filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the School filtering service must:

- Be logged in ‘change control’ logs.
- Be authorised by either the Head, Deputy Head / DSL.
- Be referred to a second responsible person prior to changes being made (as above).
- Be reported to the Online Safety Committee once every term in the form of an audit of the change control logs.

All users have a responsibility to report immediately to the Head, Deputy Head DSL any infringements of the School's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the School. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the School to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the School network, filtering will be applied that is consistent with school practice.

- The School maintains and supports the managed filtering service provided by Smoothwall.
- The School has provided enhanced / differentiated user-level filtering through the use of the filtering programme.
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head.
- Mobile devices that access the School internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the School systems.
- Any filtering issues should be reported immediately to the IT Team.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through regular online safety education. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- The Acceptable Use Agreement.
- Induction training, inset training.
- Staff meetings, briefings.

Parents will be informed of the School's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions, newsletters, letters, etc.

Changes to the Filtering System

Requests for sites to be removed from the filtered list maybe made via the helpdesk. Authorisation for this to be actioned must be given by either the Head, Deputy Head DSL, IT Team and a second person from this list informed. The IT Team will then be instructed to complete the removal. This will then be recorded on the change log by the IT Technician which is reviewed by the Technology Committee once per term.

The decision to remove a site from the filtered list will be based primarily on whether it enhances the teaching and learning or the administration in school. Checks will need to be made of links from the site. Requests of a personal nature, such as social networking sites, will be considered by the Technology Committee and could be offered on a time limited basis.

The Smoothwall filtering system monitors user activity and will flag any attempts to access inappropriate or illegal sites via email to the Head and DSL who will then investigate.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Head, Deputy Head Academic or DSL who will decide whether to make school level changes (as above).

No filtering system can guarantee 100% protection against access to unsuitable sites. The School will therefore monitor the activities of users on the School network and on school equipment as indicated in the School Online Safety policy and the Acceptable Use Agreement. Monitoring will take place as follows:

- Smoothwall monitoring user activity and records of all activity being kept for 2-3 months.
- Email is monitored.
- The DSL and Safeguarding Governor will regularly 'dip test' the system, ensuring filtering is working and the activity of users falls within the School's acceptable use.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- Senior Management and the IT Team may analyse the logs for changes made to filtering and filtering incidents once every term to detect any patterns. For example, the evidence might show a large number of requests to remove the filtering from sites – in which case schools might question whether their current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring / disciplinary action might be necessary.
- The Safeguarding Governor.
- The Technology Governor.
- The Police (on request).

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

20. Social Media

Social media (e.g.: Facebook, X, LinkedIn, Bluesky) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games and video sharing platforms such as You Tube have social media elements to them.

The School recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils/students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. Finton House encourages the safe use of social media by the School, its staff, parents, carers and pupils.

The School respects privacy and understands that staff and pupils/students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the School's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the School name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the School or impacts on the School, it must be made clear that the member of staff is not communicating on behalf of the School with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the School are outside the scope of this policy.

Digital communications with pupils/students are also considered. Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.

Roles and Responsibilities

SLT

- Facilitating training and guidance on Social Media use.
- Developing and implementing the Social Media guidance
- Taking a lead role in investigating any reported incidents.
- Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
- Receive completed applications for Social Media accounts.
- Approve account creation.

Head of Marketing, Communications and Development / IT Team

- Create the account following SLT approval.
- Store account details, including passwords securely.
- Be involved in monitoring and contributing to the account.
- Control the process for managing an account after the lead staff member has left the organisation (closing or transferring).

Staff

- Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies.
- Attending appropriate training.
- Regularly monitoring, updating and managing content he/she has posted via school accounts.
- Adding an appropriate disclaimer to personal accounts when naming the School

Process for Creating New Accounts

The School community is encouraged to consider if a social media account will help them in their work, e.g.: a history department Twitter account, or a "Friends of the School" Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:-

- The aim of the account.
- The intended audience.
- How the account will be promoted.
- Who will run the account (at least two staff members should be named).
- Will the account be open or private/closed.

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the School has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the School, including volunteers or parents.

Monitoring

School accounts are monitored regularly and frequently by the Head of Marketing, Communications and Development. Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- The School requires that all users using social media adhere to the standard of behaviour as set out in this policy and the AUA.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff

must ensure that confidentiality is maintained on social media even after they leave the employment of the School.

- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the School media policy before responding.
- Unacceptable conduct, (e.g.: defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the School and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. The School permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The School will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the School will deal with the matter internally. Where conduct is considered illegal, the School will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal Considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling Abuse

- When acting on behalf of the School, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging.
- Conversational.
- Informative.
- Friendly (on certain platforms, e.g.: Facebook).

Use of Images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the School's digital and video images policy (Section 13 of this policy). If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload pupils pictures online other than via school owned social media accounts.

- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Pupils should be appropriately dressed, not be subject to ridicule and must not be on any school list of pupils whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal Use of Social Media

Staff

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

Pupils

- Staff are not permitted to follow or engage with current or prior pupils of the School on any personal social media network account.
- The School's education programme should enable the pupils to be safe and responsible users of social media.
- Pupils are encouraged to comment or post appropriately about the School. Any offensive or inappropriate comments will be resolved by the use of the School's behaviour policy.

Parents/Carers

- If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
- The School has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on Frog VLE.
- Parents/carers are encouraged to comment or post appropriately about the School. In the event of any offensive or inappropriate comments being made, the School will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the School's complaints procedures.

Monitoring Posts About the School

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the School. This is the responsibility of the Head of Marketing, Communications and Development.
- The Head of Marketing, Communications and Development monitors all comments made by others on school social media accounts.

Policy Oversight

Policy Author/s:	Ben Freeman, Head Catherine Gomez, Deputy Head – Pastoral Andy Dyer, Assistant Head – Technology and Innovation
Policy Review date:	19 May 2026
Review Frequency:	Annual
SLT Policy Oversight:	DFO
Governing Committee:	Education
Governor Name:	Annabel Tuckey