Wellingborough School
Founded 1595

Acceptable Use of Technologies Policy (Staff)

CONTENTS

Section **Page No.**

Created: Amended	August 2016 January 2019 March 2019 November 2019	QW/PBW QW /PBW QW/PBW QW/SRM/CJS
Approved	November 2019	Whole School SLT
Next Review	November 2021	

APPROVED BY THE BOARD

Name:	**Signature:**	**Date:**

1 SCOPE OF THIS ACCEPTABLE USE POLICY

This Acceptable Use Policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all information technologies to safeguard all members of the Wellingborough School community. The policy recognises the ever-changing nature of emerging technologies and highlights the need for regular review to incorporate developments within IT.

This policy provides support and guidance to the School's Governors, Senior Leadership Team, teaching and support staff, parents/carers for the safe and responsible use of these technologies beyond the School or educational setting. It also explains procedures for any unacceptable use of these technologies by pupils or staff, and refers to School disciplinary procedures for staff and pupils

1.1 Why have an AUP?

The use of the internet as a tool to develop learning and understanding has become an integral part of School and home life. There are always going to be risks to using any form of communication which lies within the public domain. Therefore, it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst pupils access these technologies. It is also important that adults are clear about procedures, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks.

As part of the 'Keeping Children Safe in Education' (September 2019) agenda set out by the Government and the Education Act 2004, it is the duty of schools to ensure that children and young people are protected from potential harm, both within and beyond the School environment. Every effort will be made to safeguard against all risks, however it is likely that we will never be able to completely eliminate them. Any incidents that do arise will be dealt with quickly and according to this policy to ensure pupils continue to be protected.

"Prevent" is also a key part of the strategy to stop people becoming terrorists or supporting terrorism. Early intervention is at the heart of "Prevent" in diverting people away from being drawn into terrorist activity. "Prevent" happens before any criminal activity takes place. It is about recognising, supporting and protecting people who might be susceptible to radicalisation. The Prevent Strategy objectives are:

- identify individuals at risk of being drawn into terrorism;
- assess the nature and extent of that risk; and
- develop the most appropriate support plan for the individuals concerned.

Wellingborough School has systems in place that can filter, identify and record the actions of a person who frequents or accesses material that is considered as 'extremist' in nature, including the use of closed network groups, encrypted devices and browsers, suspicious contact via email, etc.

The Designated Safeguarding Lead (DSL) will consider whether a situation may be so serious that an emergency response is required and in these situations, a 999 call should be made. Where a child / young person is thought to be in need or at risk of significant harm, and/or where investigations need to be carried out (even though parental consent is withheld), a referral to the Access and Assessment Team should be made via email ***peo@northants*.pnn.police.uk** or phone **101** then extension **341166**.

1.2 Aims of the Policy

- To educate Governors, staff and parents/carers about the use of technologies both within and outside school or other educational settings.
- To provide safeguards and rules for acceptable use to guide all users in their online practices and experiences.
- To ensure adults are clear about procedures for reporting misuse of any technologies, both within and beyond the School or educational setting.

2 RESPONSIBILITIES OF THE SCHOOL

2.1 Head

The Head of each school has overall responsibility for Online Safety as part of the wider remit of safeguarding and child protection. To meet these responsibilities, the following measures are in place:

- Each School has a DSL to implement agreed policies, procedures, staff training, curriculum and take the lead responsibility for ensuring that Online Safety is addressed appropriately. All staff and pupils are aware of who holds this post within the School;
- Time and resources are provided for the DSL to be trained and to update policies, where appropriate;
- The Head promotes Online Safety across the curriculum and has an awareness of how this is being developed, in accordance with the School's Development Plan;
- The Head will inform the Governors about the progress of, or any updates to the Online Safety curriculum (via PSHCE, Life Skills or IT) and ensure they know how this relates to safeguarding;
- The Whole School SLT ensure that Online Safety is embedded within all Safeguarding Training, guidance and practices.

2.2 The Designated Safeguarding Leads (DSLs) are: R. Girling (Pre-Prep) J. Rowley-Burns (Prep), Q. Wiseman (Senior)

It is the role of the DSL to liaise with the IT Manager and vice versa, regarding Online Safety matters, in order to:

- Recognise the importance of Online Safety and understand the School's duty of care to ensure the safety of the whole school community;
- Establish and maintain a safe IT learning environment within the School;
- Update the AUP annually (or more frequently should circumstances dictate) and share these updates with staff and parents where appropriate;
- Liaise with the IT Manager to ensure the following provision is in place and sufficiently robust: firewalls, anti-virus and anti-spyware software, filters, and a system of monitoring staff and pupil use of School-issued technologies and the internet, where appropriate.
- Ensure that all staff understand how filtering levels operate and their purpose;
- Report issues and update staff on Online Safety issues on a regular basis;
- Liaise with the Heads of PSHCE, Life Skills and other relevant staff so that policies and procedures are updated and take into account any emerging issues and technologies;
- Co-ordinate or deliver staff training on Online Safety matters;

The IT Manager and SLT will further consider the following:

- Policies on using personal and school owned-devices, including mobile devices;
- Procedures for misuse, allegations of misuse or dealing with any other Online Safety issues
- An email protocol (published separately in the e-mail and communications policy)

It is the responsibility of all adults within the School to:

- Know who the DSLs are, so that any misuse or incidents involving a pupil can be reported;
- Be familiar with, or know where to access School policies in the Staff Handbook, including Safeguarding, Anti-Bullying, Disciplinary Procedures, Behaviour Policy and Code of Conduct;
- Check that websites used in lessons or specified for homework are appropriate and report any filtering concerns to the relevant designated person;
- Ensure that pupils are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner, and know what to do in the event of an Online Safety incident;
- Communicate with current pupils, and their parents/carers, via school authorised channels only **(i.e. using professional email addresses and telephone numbers).** All communications with pupils must be for School purposes only, unless otherwise authorised by the relevant Head, to minimise the risk of allegations being made against staff;
- Understand that behaviour in their personal lives may impact upon their work with pupils if/when shared online or via social networking sites;
- Ensure that if a social networking site is used privately, details are not shared with pupils, staff are advised to set privacy settings to a maximum;
- Keep usernames and passwords private and never leave work stations unattended when logged in;
- Report accidental access to inappropriate materials to the relevant DSL;

- Be mindful of transportation of sensitive pupil/colleague information and photographs on memory sticks, laptops or other devices between school and home. Encryption or password protection should be used to restrict unauthorised access in the event of loss or theft.

3 APPROPRIATE AND INAPPROPRIATE USE

To ensure that both pupils and staff are appropriately safeguarded against online risks and allegations, the latest copy of the Acceptable Use Policy is available on the School website. The policy clearly highlights any behaviours or practices, linked to staff use of technologies, which are deemed inappropriate by 'Safer Working Practice' guidelines or other relevant safeguarding legislation and professional standards. Staff are expected to take responsibility for their own use of technology and are expected to read and sign acceptance of the staff Acceptable Use of Technologies Agreement on beginning employment at the School and to acknowledge acceptance of updates. Please note that every time that you log onto to a school device or use your own device that is connected to the school Wi-Fi, you are agreeing to the AUP.

Examples of inappropriate use:

- Accepting or requesting current and recent (within the last 3 years) pupils as 'friends' on social networking sites, or exchanging personal email addresses or personal mobile phone numbers.
- Behaving in a manner which would lead any reasonable person to question a staff member's suitability to work with children or act as a role model. This would include inappropriate comments, photographs or videos on social networking sites which reflect badly on either the individual, their colleagues or the School/workplace.

In the event of inappropriate use

5

If a member of staff is believed to misuse the internet or network in an illegal, inappropriate or abusive manner, a report must be made to the relevant Head / DSL immediately and the Online Safety Incident Flowchart referred to (see appendix). If necessary, the appropriate Local Safeguarding Children's Partnership (LSCP) allegation procedures and safeguarding policies must be followed to deal with any misconduct and all relevant authorities contacted. In the lesser event of minor or accidental misuse, internal staff disciplinary procedures, as set out in the Staff Handbook, will be referred to in terms of any action to be taken.

4 THE CURRICULUM

4.1 Internet use

It is the responsibility of schools to teach their pupils how to use the internet safely and responsibly. The following concepts, skills and competencies will continue to be developed through both the PSHCE and IT curriculum:

- Internet literacy
- Making good judgements about websites and emails received
- Knowledge of risks such as viruses and opening mail from a stranger
- Knowledge of copyright and plagiarism issues
- File-sharing and downloading illegal content
- Uploading personal information – what is and is not safe
- Where to go for advice and how to report abuse - CEOP
- The storing of School created content online – where to and where not to

Online personal safety is taken extremely seriously within our School community and our pupils are encouraged to refrain from sharing personal information in any form of electronic communications. Personal information includes:

- Full name
- Address
- Telephone number
- Email address
- School
- Clubs attended and location
- Age or Date of Birth
- Parent names

4.2 Email use

Only School email address using the @wellingboroughschool.org domain name should be used for all electronic correspondence between staff and pupils. This is true also for any communications with parents or recent (within the last 3 years) pupils. If in doubt on this last issue a member of staff is advised to speak to a member of the relevant SLT. Under no circumstances will staff members engage in personal communications (e.g. via social media) with current pupils or parents outside authorised School systems. The use of School email accounts allows for content monitoring to take place and minimises the risk of allegations being made against staff and council members.

4.3 Mobile technologies

Everyday technologies, including but not restricted to mobile phones, smart watches and laptop/tablet computers are used by both adults and pupils within the School environment. For this reason, appropriate safeguards must be in place to protect young people and staff.

i) Mobile phones and Smart Watches

Staff may bring personal mobile phones and smart watches into school, but they will be used outside lesson time only and in a discreet manner. Under no circumstances should staff use their personal accounts to communicate with current or former pupils or their parents/carers. The School recognises that members of staff who are also current parents have a different set of parameters, but they must act at all times in a professional manner. All images or video recordings of children and young people should be taken using school equipment as far as possible. Any photographs taken on personal devices must be transferred appropriately and as soon as possible; the original image should be deleted from the device and from any related cloud-based locations if automatically transferred. It is the responsibility of staff to ensure that no inappropriate or illegal content is stored on their device when bringing it onto school grounds.

ii) Laptop/tablet computers, USB sticks & Cloud-Based Storage

Staff are permitted to access the school Wi-Fi and network resources on personal devices, providing sensitive data is not kept upon the equipment. In the event that a laptop is stolen or lost there is potential for this content to be viewed by unauthorised individuals. This applies also to the use of memory sticks for transferring information between school and home, which should be encrypted. Staff should only use the school administered Office365 OneDrive cloud-based storage for storing sensitive data, not any other cloud-based storage such as Dropbox.

4.4 Video and photographs

While it is recognised that the use of photography is as an important opportunity to add colour, life and interest within the School, all imagery must always be used in a responsible way. As photographs are considered to be personal data, both the 'Keeping Children Safe in Education' guidelines and the Data Protection Act 2018 regulations must be observed. Therefore the need to respect both pupils' and parents' rights of privacy and be aware of potential child protection issues must always be taken into account when taking photographs.

To meet these responsibilities, the School has the following measures in place:

- Images or videos featuring pupils will only be used if consent has been given by parents. There are four categories of consent, and parents can choose to either consent to one or more of the categories or to all of the categories:

1.	2.	3.	4.
Use of photographs of their child in and around school, in places that might be seen by visitors	**The school using photographs of their children on the school website**	**The school using photographs of their child on social media**	**The school using photographs of their child in wider marketing materials used by the school**

- Photograph consent can be withdrawn at any time and parents can do this by emailing data@wellingboroughschool.org, also parental photograph consent will be checked each year as part of the data collection checking process
- Digital images of pupils must be stored in a way that they can deleted in entirety and they should not be kept for longer than is necessary for their original purpose
- The School must keep control of all digital images taken by staff or pupils. Therefore school equipment should be used and USB sticks, camera storage cards, etc. must be kept onsite and securely stored, wherever possible
- Staff should, as much as possible, ensure that images of pupils cannot be viewed by unauthorised individuals and prevent their loss or theft; therefore images should be removed from cameras, iPads, etc. and utilised appropriately as soon as practically possible
- Wherever possible group shots of pupils will be taken, as opposed to images of an individual and **only first names can be displayed**
- Photographs should not show pupils in compromising positions or in inappropriate clothing and settings. (E.g. toilets, changing rooms, swimming pool, etc.)

4.5 Tapestry

In the Foundation Stage – Nursery and Reception – the School is legally required to make and share a learning profile for every child with their parent/guardian. The profile shows the progress of each child through their time in the Foundation Stage through observations, photographs, videos and children's work.

The School uses a program called Tapestry to assemble and create the learning profile. This is in the form of an online learning journal, which helps track, record, assess and celebrate the children's progress throughout the Foundation Stage with parents and members of the Foundation team. All teachers and teaching assistants in the Pre-Prep have their own passwords to the software, and are able to contribute to individual profiles.

The journals are the property of the School and Tapestry cannot access individual profiles. We have a legal requirement to share the information with our parents; which is now shared securely with parents through Firefly, alongside a letter stating that parents 'do not share the photos on social media or use the photos inappropriately'. School iPads and iPods are always used to take photos, as per the School's policy. Tapestry has a security policy of its own, which can be viewed at any time.

4.6 Video-conferencing, 'Facetime', 'Skype' and webcams

To safeguard staff and pupils, publicly accessible webcams are not to be used in school to communicate with a third party unless explicit permission is given by parents/carers. Video communications with individuals or groups outside of the School setting (e.g. communicating with a school overseas) must always be supervised by staff and a record of dates, times and participants held in school for audit trail purposes.

5. SOCIAL MEDIA

5.1 Managing Social Media

Social networking is now the communication form of choice for many adults and young people worldwide and, as a result, safeguards must be in place to ensure that pupils are aware of the risks associated with this form of technology.

To address this issue, a series of preventative measures are in place:

- Access to social networking sites is restricted through the School internet filtering systems;
- Pupils are discouraged from providing personal details or identifiable information on profiles (e.g. mobile number, address, School name, clubs attended, email address or full names of friends);
- Pupils are made aware of the risks of posting images online and how publicly accessible their content is. Background images in photographs which may reveal personal details are also addressed (e.g. house number, street name, School uniform);

- Social networking security settings are explained and recommendations made for privacy settings to be activated to 'Friends only' for all applications to restrict unsolicited access. The importance of passwords and blocking of unwanted communications is also highlighted in Life Skills and PSHCE sessions;
- Both national/online (e.g. CEOP) and school systems for reporting abuse or unpleasant content, i.e. cyberbullying, are taught and reinforced regularly.

5.2 Staff using social networks

Social networking outside of work hours, on non-school equipment, is the personal choice of all school staff. Owing to the public nature of such websites, staff have a responsibility to ensure that their actions outside school do not impact on their work with children and young people. The 'Keeping Children Safe in Education' & 'Safer Working Practice' guidelines clearly state that adults working with children should:

- Ensure that if a social networking account is used, privacy settings are set to maximum. If staff are unclear how to do this they should seek advice;
- Staff should not accept or request current and recent (within the last 3 years) pupils as 'friends' on personal social networking sites, or exchange personal email addresses or personal mobile phone numbers;
- Be aware that behaviour in their personal lives may impact on their work with children and young people;
- Be aware that their professional obligation is to the School, as their employer, and so they must exercise caution over any postings which might bring the School into disrepute or are critical of the School;
- Not behave in a manner which would lead any reasonable person to question their suitability to work with children and young people;
- Be aware that information posted on such sites is potentially accessible to a wider audience and that staff should take care to safeguard their own and the School's reputation. If inappropriate comments are made, the School may decide to take disciplinary action.

6. SAFEGUARDING MEASURES

6.1 Filtering

Internet access in the School is filtered through the iBoss platform, with additional family/safe search settings enabled. Impero software is used to monitor and manage all network activity. To safeguard young users from viewing inappropriate content, all filtering is set to high and then individual access controlled via local blacklists which limit access to specific websites, categories of websites and a custom 'restricted list'.

In addition to the above, the following safeguards are in place:

- DSLs will periodically carry out checks on the School's filtering system to ensure that pupils are not able to access inappropriate sites. IT Support will provide a termly report to confirm that appropriate filters are in place, and will report any attempted bypassing of the system to the DSLs immediately;
- A firewall secures sensitive data from unauthorised users;
- Pupils use a search engine that is set to high levels of moderation and where possible, age appropriate search engines such as https://www.safesearchkids.com/ or http://www.primaryschoolICT.com
- Pupils know where the **Child Exploitation and Online Report (CEOP**) button is located (on the pupil splash screen in a web browser and on the Pupil Firefly Dashboard) and are encouraged to report any concerns of inappropriate or malicious contact made by another user. This provides a safe place for children and young people to report an incident if they feel they cannot talk to a trusted adult.

6.2 Tools for bypassing filtering

The use of VPNs (virtual private networks) or any other technology designed to circumvent, avoid or bypass security controls (including internet filters, antivirus solutions or firewalls) within school is **strictly forbidden.** A VPN is capable of hiding the IP address of the user and opening unrestricted and, in cases, unidentifiable channels through which blocked material can be viewed e.g. Social networking sites, gaming websites or adult content. Violation of this rule by pupils will result in school sanctions being applied.

7. SUPPORT

As part of the School's approach to developing Online Safety awareness with pupils, every effort is made to offer parents/carers the opportunity to find out more about how they can support their son/daughter to stay safe online within and beyond the School environment. Online Safety parent/carer Information sessions are held to raise awareness of key internet safety issues and highlight safeguards currently in place at school. Free resources and information to support parents can also be found on Childnet (https://www.childnet.com/parents-and-carers) and ThinkUKnow (https://www.thinkuknow.co.uk/parents)

8. LINKS TO OTHER POLICIES

8.1 Behaviour, Cyberbullying and Anti-Bullying

The Acceptable Use Policy is cross-referenced by a number of other School policies, including those for Behaviour, Anti-Bullying, PSHCE, Safeguarding and the Data Protection Policy. Cyberbullying features within the School's Anti-Bullying Policy due to the growing number of incidents recorded. Cyberbullying will not be tolerated in or outside School and clear procedures for dealing with cyberbullying incidents can be found within the Anti-Bullying Policy.

8.2 Managing allegations and concerns of abuse made against people who work with children.

Allegations made against staff members must be reported to the relevant DSL within school immediately. In the event of an allegation being made against the Head, the Chair of Governors will be notified immediately.

8.3 PSHCE

The teaching and learning of Online Safety is embedded within the PSHCE, Enrichment and Life Skills curriculum, in all parts of the School, to ensure that the key safety messages about engaging with people are the same whether pupils are on or offline.

8.4 CCTV

The Data Protection Act 2018 and the Information Commissioner's CCTV Code of Practice state that all Schools using CCTV for security and safety purposes must publicly declare that they are doing so. Signs have been erected to inform members of the public that they are entering a surveillance area.

Where possible, images recorded through the CCTV system are fully traceable with the date, time and device detailed in a secure log for audit trail purposes. A robust collection of Standard Operating Procedures are in place to govern the day to day operation of the CCTV system. For data security purposes a restricted number of staff can access any images and recordings held by the School.

8.5 School website and Twitter feed

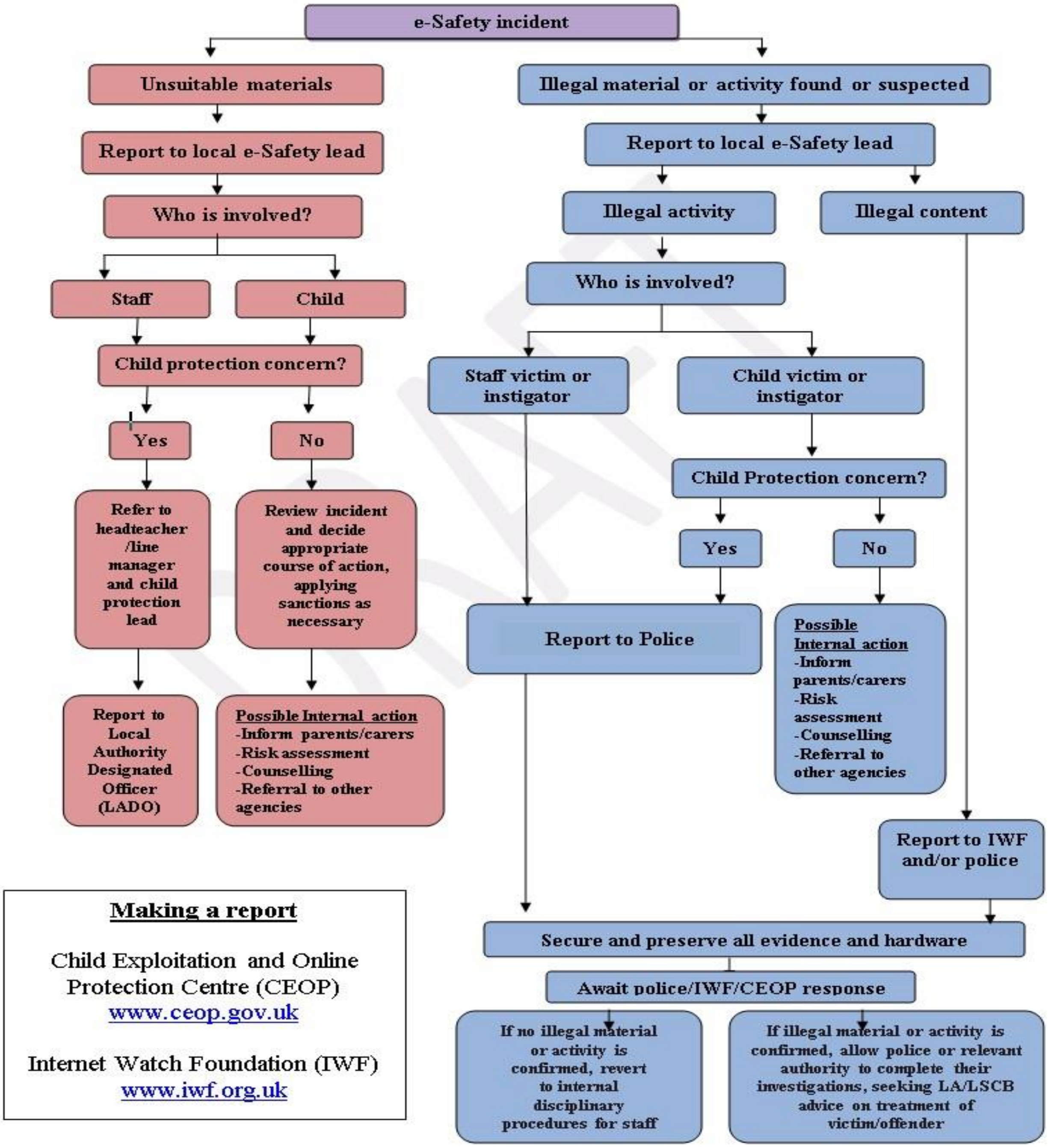
Permission will be sought from parents/carers prior to the uploading of any images onto the School website or Twitter feed. Consideration is given to which information is relevant to share with the general public on a website and secure areas will be used for information pertaining to specific audiences.

8.6 Disciplinary Procedure for Staff

In the event that a staff member is seen to be in breach of professional standards of conduct or is believed to have misused online technologies, School disciplinary procedures will be followed as laid out in the relevant Staff Handbook.

Appendix 1

Incident Flow Chart


e-Safety incident
Unsuitable materials
Report to local e-Safety lead
Who is involved?
Staff
Child
Child protection concern?
Yes
No
Refer to headteacher /line manager and child protection lead
Review incident and decide appropriate course of action, applying sanctions as necessary
Report to Local Authority Designated Officer (LADO)
Possible Internal action -Inform parents/carers -Risk assessment -Counselling -Referral to other agencies
Illegal material or activity found or suspected
Report to local e-Safety lead
Illegal activity
Illegal content
Who is involved?
Staff victim or instigator
Child victim or instigator
Child Protection concern?
Yes
No
Report to Police
Possible Internal action -Inform parents/carers -Risk assessment -Counselling -Referral to other agencies
Report to IWF and/or police
Secure and preserve all evidence and hardware
Await police/IWF/CEOP response
If no illegal material or activity is confirmed, revert to internal disciplinary procedures for staff
If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations, seeking LA/LSCB advice on treatment of victim/offender

Making a report

Child Exploitation and Online Protection Centre (CEOP)
www.ceop.gov.uk

Internet Watch Foundation (IWF)
www.iwf.org.uk

*** e-Safety L:eads - Designated Safeguarding Leads (DSL's) are.**

APPENDIX 2

Serious incidents affecting safeguarding

There are three instances when the School must report directly to the police:

- Indecent images of children found
- Incidents of 'grooming' behaviour
- The sending of obscene materials to a child.

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found. The police will advise on how to deal with the machine if they are unable to send out a forensics team immediately. If in doubt, do not turn off the machine. The Internet Watch Foundation www.iwf.org.uk offers further support and advice in dealing with offensive images online.

It is important to remember that any offensive images received should never be forwarded, even if it is to report them as illegal, as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.

Wellingborough School Filtering Change Log

Any change filtering levels whether temporary or permanent can only be considered through a written request to the Manager of Information Systems. This is recorded and sanctioned by the senior DSL before the change is made.

Example of filtering log format

Website / category	Date	Requested by/ reason	Authorised by	Change made by	Confirmed by	Date for review
www.example.com	01/10/19	Website used to support study of Ancient Greek A Level. Strong language but is appropriate to age group.	CJS (IT Manager)	TPC (Senior IT Technician)	QIW (Deputy Head and DSL)	31/10/19

Wellingborough
School
Founded 1595

Staff Acceptable Use of Technologies Agreement

To ensure that **all** staff are confident in their use of technologies and the internet, this Acceptable Use of Technologies Agreement and accompanying Acceptable Use Policy (AUP) has been developed in collaboration with education professionals and unions.

The core values of the Acceptable Use Policy are safeguarding and responsible behaviours allowing young people, and the adults who surround them, to enjoy all the benefits that technology can offer. To assist with this, the full Acceptable Use Policy is accessible to all staff members and should be referred to for further information.

The Designated Safeguarding Leads are Qin Wiseman, Jo Rowley-Burns and Rebecca Girling, and the principle IT contact is Colin Summers.

All staff need to understand:

- School equipment and the network must always be used in an appropriate manner;
- Staff must not have personal communications with current and recent (within the last 3 years) pupils, outside of their professional role. This includes establishing social networking 'friendships' on sites such as Facebook, or sharing personal phone numbers or email addresses. Any School related communication must be conducted through professional email accounts or telephone numbers only;
- Staff should not behave in a manner, either **within or outside** of the work environment, which would lead any reasonable person to question their suitability to work with children or act as a role model. This would include inappropriate comments, photographs or videos on social networking sites which reflect badly on themselves, colleagues or the School;
- Permission must be received from parents/carers before images of children are used online (e.g. School website or the School's Twitter feed). Images must be appropriate and should not reveal any personal information;
- Staff may bring personal mobile phones and smart watches into school, but they will be used outside lesson time only and in a discreet manner. Under no circumstances should staff use their personal accounts to communicate with current or former pupils or their parents/carers. The School recognises that members of staff who are also current parents have a different set of parameters, but they must act at all times in a professional manner. All images or video recordings of children and young people should be taken using school equipment as far as possible. Any photographs taken on personal devices must be transferred appropriately and as soon as possible; the original image should be deleted from the device and from any related cloud-based locations if automatically transferred. It is the responsibility of staff to ensure that no inappropriate or illegal content is stored on their device when bringing it onto school grounds.

- Any incidents of concern for children's safety must be reported to the relevant DSL, in accordance with procedures listed in the Acceptable Use Policy;
- All staff know where to access a copy of the Online Safety Incident Flowchart should an incident of misuse arise;
- The School email system and all School issued devices are routinely monitored as part of our commitment to safeguarding;
- Each user should be accessing the internet with their unique username and password for filtering and safeguarding purposes. For this reason, passwords must be kept private;
- **Any concerns regarding School IT use must be flagged to line managers or the DSLs to avoid possible misunderstandings;**
- All Staff have access to the full Acceptable Use and Social Media Policies on the School website, should they need to refer to these documents about any Online Safety issues or procedures.

I have read, understood and agree to the above IT Acceptable Use Rules, and understand that these rules are in place to ensure that staff are aware of their professional responsibilities to safeguard children when accessing online technologies to protect pupils and staff. I understand that every time I log onto to a school device or use my own device that is connected to the school Wi-Fi, I am agreeing to the AUP.

Signed ……………………………………………………………………………….. Date …………………………………

Name (printed) ………………………………………………