WINDERMERE SCHOOL
FOUNDED 1863

Windermere School ONLINE SAFETY POLICY

This Policy is applicable to all pupils, including those in the Early Years Foundation Stage.

Windermere School Safeguarding Policy

This Policy is applicable to all pupils, including those in the Early Years Foundation Stage.

Review Date: August 2026

Reviewed by: SLT and Governors

Review Period: 12 months (and ongoing)

Staff Responsibility: Head of Safeguarding and Wellbeing

Development, Monitoring and Review of this Policy

This Online Safety policy will be developed, monitored and reviewed by Windermere School's Online Safety Group made up of:

- A member of the Governing Body i/c of safeguarding – Mr Peter Hogan
- Online Safety Coordinator – Mrs Susan Brown
- Member(s) of the Senior Leadership Team/Designated – Jenny Davies, Lynn Moses, Susan Brown
- Technical ICT staff – Network Manager – Arron Wakefield
- Operations Director - Andrew Smith

Consultation with the whole school will periodically take place through a range of formal and informal meetings and be presented to the group by the most appropriate people.

Parents, community advisors and pupils can be co-opted onto the group when necessary.

Schedule for Development, Monitoring and Review

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring of data for network activity
- Surveys and questionnaires of
- Pupils
- Parents/carers
- staff
-

Scope of the Policy

Windermere School and Windermere Summer School (henceforth referred to as "the School" unless specific arrangements apply) are fully committed to ensuring that the welfare of all children and is their main priority. This includes children aged three to 11, who are in Prep or Pre-Prep (referred to hereafter as Prep School). For the purpose of this policy, children includes everyone under the age of 18.

This policy applies to all members of the Windermere School this includes staff, pupils, volunteers, parents/carers and visitors who have access to and are users of school ICT systems, both in and out of the School.

The School recognises that issues that can affect online safety is vast and ever changing, but that the four key areas of risk are:-

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or

young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

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

commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti Phishing Working Group

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

The School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. The role of the Online Safety Governors will include:

- regular meetings with the Online Safety Co-ordinator
- regular monitoring of online safety incident logs
- regular monitoring of filtering logs

- reporting to relevant Governors

Head and Senior Leadership Team

- The Head has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Co-ordinator.
- The Head and (at least) another member of the Senior LeadershipTeam 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.
- The Head and Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as neccessary This also includes the sharing of information to the ICT Team.
- The Head and SeniorLeaders 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.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.

Online Safety Coordinator:

The roles and responsibilities of the online safety coordinator include:

- being up-to-date with their own online safety training
- leading the Online Safety Group.
- taking day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policy.
- 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 regularly with Online Safety Governor(s) to discuss current issues, review incident logs and filtering.

- attending relevant meetings to report to Governors.
- reporting regularly to the Senior Leadership Team.

Incidents which breach the online Acceptable Use Policy will be dealt with through the School Expectations and Contract for Pupils. The Online Safety Coordinator will discuss such incidents with the DSLs and Deputy Head in line with the policy to decide actions to be taken. If deemed necessary, educational restorative sessions will be put in place for the pupils involved and any others who could be affected by any incidents. This will normally be carried out by the Online Safety Coordinator in conjunction with appropriate members of the Pastoral team.

Technical ICT staff:

The Technical staff are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the School meets required online safety technical requirements and any other Online Safety Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- the filtering protocol is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- through the Line Manger they are informed of online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant. Information will also be shared from third parties where relevant and cascaded by the Line Manager.
- that the use of the network, internet, remote access and emails is regularly monitored in order that any misuse or attempted misuse can be reported to the Online Safety Coordinator for investigation.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current Online Safety Policy and practices.
- they have read, understood and signed the ***Device Policy***.
- they report any suspected misuse or problem to the Online Safety Coordinator, or if they are not available, a member of the Senior Leadership Team for investigation.
- all digital communications with pupils, parents/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.
- pupils understand and follow the Online Safety Policy and acceptable use policies.
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Leads

Our Designated Safeguarding Leads are trained in Online Safety issues and are aware of the potential for serious child protection or safeguarding issues to arise from:

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

The DSLs are responsible for ensuring that age-appropriate education is in place through the Life Skills programme and general Pastoral Education to ensure pupils know how to protect themselves when they are online.

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from Windermere School and outside agencies, when required. They have responsibility for issues regarding online safety and the monitoring of the Online Safety Policy including the impact of any new initiatives. The group is responsible for regular reporting to the Governing Body through the Online Safety Governor and the Online Safety Coordinator.

Members of the Online Safety Group will assist the Online Safety Coordinator with:

- the development, review and monitoring of the school Online Safety Policy and other related documents.
- the production, review and monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.
- mapping and reviewing the online safety curricular provision through the Life Skills programme – ensuring relevance, breadth and progression
- monitoring network and internet incident logs
- consulting stakeholders – including parents/carers and the pupils about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking or use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the School's Online Safety Policy covers their actions out of school, if related to their membership of the School.

Parents/Carers

Parents and carers play a crucial role in ensuring that their children 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' meetings and regular newsletters containing the most up-to-date advice. 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
- their children's personal devices in the school and at home.

This is not an exhaustive list.

Policy Statements

Education – Pupils

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

In order to consider the quantity of safeguarding concerns online, the government published guidance Teaching online safety in schools. This publication outlines the importance of online safety but also, gives guidance to pupils on how to behave online. This can be read in conjunction with Education for a Connected Worls Framework (UKCIS), which offers age specific advice about online knowledge and skills. This guidance assists with looking at the many areas of a curriculum where online safety could be taught, and focuses on the following underpinning areas:-

- How to evaluate what pupils see online.
- How to recognise techniques used for persuasion.
- Online behaviour.
- How to identify online risks.
- How and when to seek support.

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

- A planned online safety curriculum should be provided as part of Computing, ICT and Life Skills plus other lessons when relevant and this should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies, reflections and tutorial activities.
- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Pupils should be supported in building resilience to radicalisation by the provision of a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils can freely search the internet, staff should be vigilant in monitoring the content of the websites the pupils visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g., racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Technical Support Team can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be recorded, with clear reasons for the need.

Education – Parents/Carers

Many parents and carers may have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Windermere School will therefore seek to provide information and awareness to parents and carers through:

- Newsletters and social media posts with reference to relevant websites or publications.
- Parent Advice Meetings offered on a yearly basis.
- Making campaigns and events such as Safer Internet Day high profile to encourage conversation.

Education & Training – Staff and Volunteers

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school's 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 Online Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings and INSET days.
- The Online Safety Coordinator will provide advice, guidance and training to individuals as required

Training – Governors

Governors should take part in online safety training and awareness sessions, with particular importance for those who are members of the Online Safety Group. Normally this will be offered through participation in School training, information sessions to parents or bespoke governor training led by the Online Safety Coordinator.

Technical – infrastructure, equipment, filtering and monitoring

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

- School technical systems will be managed in ways that ensure that the school protects the pupils in line with advice from the KCSIE (Keep Children Safe in Education).

- 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.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the ICT Technical team who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every term.
- The “master or administrator” passwords for the school ICT system, used by the ICT Technical Support Team must also be available to the Head or other nominated senior leader and kept in a secure place.
- The Operations Director has overall responsibility as Line Manager for the IT Department.
- The Operations Director 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.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC (Child Abuse Image Content) list. Content lists are regularly updated, and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The School has provided differentiated user-level filtering, allowing different filtering levels for different stages and different groups of users – staff, pupils etc.)
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the ***Device Policy***
- Users can report any actual or potential technical incident or security breach to the Online Safety Coordinator using the ICT Incident or Near Miss form.
- 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 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.
- Through the Staff Code of Conduct expectations regarding the extent of personal use that staff and their family members are allowed on school devices will be outlined.
- Through the Staff Code of Conduct expectations are described regarding the use of removable media (e.g., memory sticks, CDs, DVDs) by users on school devices.

It should be noted that personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Artificial Intelligence

Artificial Intelligence (AI) and Safeguarding.

The role of the DSL and Senior Leaders is to identify and respond to risk where children could come to harm through AI, and The School looks at the four steps of AI readiness:-

Developing Awareness: recognising AI as a safeguarding issue

Understand Risk:- Identify and naming AI related harms (ie deepfakes, sextortion).

Integration:-embedding AI and associated safeguarding threats inro policies, training and procedures.

Leadership:- Ensure that School leadership embeds a culture that safeguards from AI risk.

The Department has published Generative AI: product safety expectations to support schools to use generative artificial intelligence safely, and explains how filtering and monitoring requirements apply to the use of generative AI in educationhttps://www.gov.uk/government/publications/generative-ai-product-safety-expectations/generative-ai-product-safety-expectations

The Manosphere and Incel Culture

The manosphere refers to a collection of online communities that support and promote stereotyped, adverse or misogynistic views regarding gender roles. These communities range from those that are seemingly innocuous, spaces where men's issues are discussed to the more extreme spaces and advocate hostility and violence against women. Adolescents, especially boys are vulnerable to theses groups. At face value, some manosphere content appears as fitness advice, financial guidance or motivation, but can quickly lead to a hostile belief system about females, relationships and social power. The manosphere incudes a range of groups including:-

Incels (involuntary celibates): An online subculture of mostly male heterosexuals who believe that they cannot find a romantic or sexual female partner despite wanting one and blame females for this position.

Red Pill: A belief that wants to expose the 'truth' that society is built against men and that women are naturally manipulative.

Black Pill: An anarchic strand of red pill ideology that believes that men will always fail and nothing can be done to alter this.

Men Going Their Own Way (MGTOW): Having decided that women are worth neither the effort nor the risk, men completely disconnect entirely from relationships with females.

Pick-Up Artists (PUAs):In viewing women as targets that should be conquered, a teaching method that promotes coercion and manipulation, to gain sexual access to females.

Tradwife and Influencer Culture: A belief that reinforces regressive gender roles, promoting submission under the disguise of traditional values.

Manosphere content tends to be found on platforms with minimal oversight,and can lead to algorithms that feed to increasingly extreme content. Teenage boys are at particular risk. They are more susceptible to rigid thoughts and to seemingly knowledgeable and charismatic opinions that give a sense of belonging as they are at a developmental stage of life, with the brain is preparing to;

- Question and form identity
- Seek peer approval and status
- Take additional risks and freedoms increase
- Compare self with peers
- Develop strong emotional responses

Manosphere is a safeguarding concern, responses as it can lead on to additional issues such as:

- Normalising coercion, control and relationship hostility
- Greater possibility of developing mental health issues such as anxiety, low self-worth and social withdrawal
- Isolation and greater involvement in online subcultures reinforcing harmful beliefs
- Perceive violence or dominance as acceptable
- Form unhealthy attitudes to physical appearance/social status

Such belief systems are addressed through ongoing education, that aims to foster healthy attitudes to online safety, whilst supporting personal development. Issues highlighted as cause for concern are discussed with relevant staff, including The Wellbeing Team.

Given that some manosphere ideologies overlap with extremist narratives, The School is mindful to consider concerns in line with their Prevent duty.

Looxsmaxxing and Body Image

Although historically focused on girls, and increasing number of boys appear to be engaging in online trends promoting extreme appearance enhancement. This trend can be rooted in manosphere ideals, particularly dominance and attractiveness. It is also known as:

Looksmaxxing: pursuing the maximum attractiveness possible-often associated with toxic masculinity ideals and non-scientific suggestions.

Overgrooming: Obsessively managing overall appearance accompanies with perfectionism, shame and anxiety.

Permissions to Adjust Filtering

In order to adjust the filtering of the firewall,Sophos, all staff and students must follow procedure to ensure that any adjustments are made safely and with good reason. This procedure will see all requests go through an approval process where DSLs, the Network Manager and academic staff screen and approve all requests.

Procedure for staff when requesting filter adjustments:

- Staff have departmental meetings every two weeks. During these meetings adjustment of filtering will be an agenda item.
- Requests will then be submitted to IT Support. The request will then go through an approval process before any filter adjustments are made.

Procedure for students when requesting filter adjustments:

- Students will have to complete a ticket with the necessary paperwork in order to request the adjustment of the filter.
- This request will then go through an approval process.

Mobile Technologies

Mobile technology devices may be school owned or personally owned and might include smartphones, tablets, laptops 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 the school's learning platform and other cloud-based services such as email and data storage.

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

- **The School Acceptable Use Agreements for Pupils and Parents/Carers will consider the use of mobile technologies.**

The School allows:

	School Devices		Personal Devices		
	School owned for single user	**School owned for multiple users**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	Yes	Yes	Yes Years 7-11 are not permitted their mobile phones during the working day, unless approved by a teacher for educational	Yes	Yes

			purposes. Phone should be locked in a pouch.		
Full network access	Yes	Yes	No	No	No
Internet only			Yes	Yes	Yes limited through Guest log in
No network accesses					

Use of digital and video images

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

Windermere School will inform and educate users about these risks and this policy is intended to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g., on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website, on social media or in the local press
- In accordance with guidance from the Information Commissioner's Office, parents/ carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents/ carers comment on any activities involving other pupils in the digital images.

- Staff and volunteers can take digital or video images to support educational aims, but must follow Windermere School's protocol concerning the sharing, distribution and publication of those images, (see the School's Photography and Images policy). Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes under normal circumstances but if a personal device must be used, permission must be sought from a member of the SLT, the images must be downloaded onto a School device as soon as possible and then deleted from the personal device.
- Care should be taken when taking digital images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupils' work can only be published with the permission of the pupil and parent or carer if deemed necessary.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations Act 2018 (GDPR) which states that personal data must be:

- Fairly and lawfully processed in a transparent manner
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The School must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the “School Privacy Notice and Guide” and lawfully processed in accordance with the “Data Retention Policy”.
- It has a Data Protection Policy detailed in the School Privacy Notice and Guide
- Data Impact assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage/cloud computing which ensure that such data transfer/storage meets the requirements laid down by the Information Commissioner’s Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted, and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

This is an area of rapidly developing technologies and uses. Schools/academies will need to discuss and agree how they intend to implement and use these technologies. Windermere School do not allow casual access to mobile phones for pupils from Early Years to Year 11 between 8.30am and 4.00pm (home time for pupils below Year 7) but pupils can use their devices if permitted by a member of staff for educational purposes.

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies Windermere 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.
- Users must immediately report, to the Online Safety Coordinator – in accordance with the School policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (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.
- Whole class/group email addresses may be used but all pupils from Year 1 upwards will be provided with their own personal School email address.
- 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.

Social Media – Protecting Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly, for acts of their employees in the course of their employment. 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. Reasonable steps to prevent predictable harm must be in place.

Windermere 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; reporting issues.

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or staff.
- They do not engage in online discussion on personal matters relating to members of the School community.
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

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

- A process for approval by Senior management or appropriate staff as designated by senior management.
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff.
- A code of behavior for users of the accounts, including:
  - Systems for reporting and dealing with abuse and misuse.

Personal Use:

- Personal communications are those made via a personal social media account. 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.
- 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.

Monitoring of Public Social Media

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

The School's use of social media for professional purposes will be checked regularly to ensure compliance with the School policies.

Unsuitable or inappropriate activities

Some internet activity e.g., accessing child abuse images or distributing racist material is illegal and is therefore banned from School and all other technical systems. Other activities e.g., cyber-bullying would be banned and could lead to criminal prosecution.

There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

Windermere 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.

Responding to incidents of misuse.

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

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the LSCB (Local Safeguarding Children's Board) and if deemed necessary 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 or irresponsible or, very rarely, through deliberate misuse.

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

  - Internal response or discipline procedures.
  - Involvement by Local Authority or appropriate external organisation if deemed relevant.

- Police involvement.

- **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 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. The completed form should be retained by the group for evidence and reference purposes.

Windermere School Actions & 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.