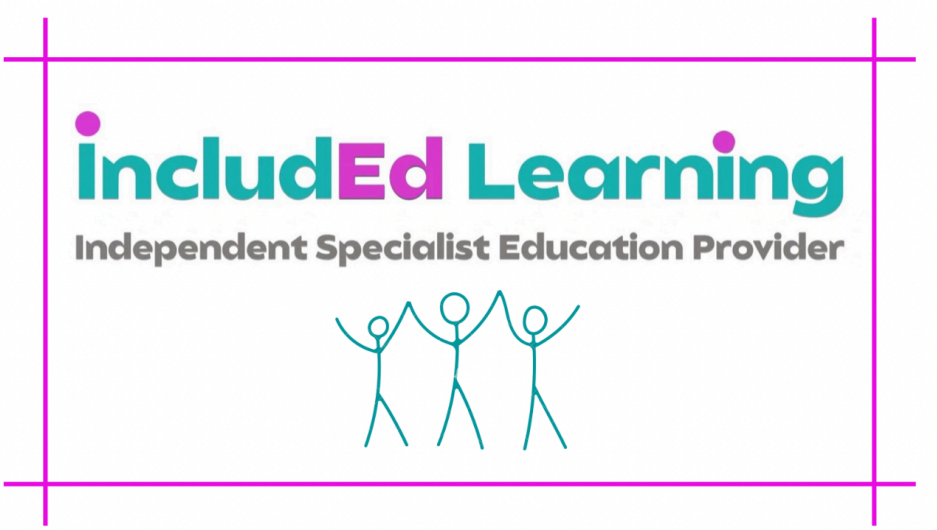

ONLINE SAFETY POLICY

Essential Safeguarding Information

KEEPING CHILDREN SAFE IN EDUCATION

We will adhere to the advice regarding all aspects of online safety including filtering and monitoring standards.

See KCSiE Keeping Children Safe in Education 2023

This online safety policy is linked to our:

- ☐ Child protection and safeguarding policy
- ☐ Behaviour policy
- ☐ Staff disciplinary procedures
- ☐ Data protection policy and privacy notices
- ☐ Complaints procedure

Author	N. Khan
Date agreed by Advisory Panelning Body	October 2023
Review Date	October 2024
Signature	

Contents

1. Policy Aims	p.4
2. Legislation and Guidance	p.5
3. Scope	p.6
4. School Ethos and Culture	p.7
5. Cyberbullying	p.9
6. Education and Training	p.10
7. Filtering and Monitoring	p.16
8. Monitoring Arrangements	p.20
Appendix 1: Communications	p.21
Appendix 2: Unsuitable Inappropriate Activities	p.23
Appendix 3: Incidents : Pupils	p.24
Appendix 4: Incidents - Staff	p.22
Appendix 5: Acceptable Use Internet - Pupils	p.23
Appendix 6: Acceptable Use Internet - Staff	p.24
Appendix 7: Online Safety Training Needs Staff Self-Audit	p.31
Appendix 8: Online Safety Incident Report Log	p.32

➔ 1. Policy Aims

At IncludEd Learning, we are committed to the high quality use of ICT to enhance and enrich our curriculum. Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and Advisory Panelnors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.

- **Contact** – being subjected to harmful online interaction with other users, such as 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** – personal online behaviour that increases the likelihood of, or causes, harm, such as 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.

➔ 2. Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- ➔ Teaching online safety in schools
- ➔ Preventing and tackling bullying
- ➔ cyber-bullying: advice for headteachers and school staff
- ➔ Relationships and sex education
- ➔ Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study. This policy complies with our funding agreement and articles of association.

➔ 3. Scope

This policy applies to all members of the school community (including staff, pupils, advisory panel members, volunteers, parents/carers and visitors) who have access to and are users of school IT systems, both in and out of school. The Education and Inspections Act 2006 empowers Headteachers, to 3 such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform partner schools and parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

➔ 4. School Ethos and Culture

This section outlines the roles and responsibilities for e-safety of individuals and groups within the school.

Advisory Panel
The Advisory Panel are responsible for the approval of the e-safety policy and to Quality Assure the policy.

Head of Centre
The Head is responsible for ensuring: The safety (including e-safety) of all members of the school community, although the day to day responsibility for e-safety may be delegated to the E-Safety Coordinator - adequate training is provided and effective monitoring systems are set up. That relevant procedure in the event of an e-safety allegation are known and understood. Establishing and reviewing the school e-safety policies and documents (in conjunction with e-safety coordinator) The school's Designated Safeguarding Lead should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise through the use of IT.

E-Safety/ICT Coordinator
The E-Safety Coordinator takes day to day responsibility for e-safety issues and has a leading role in: Liaising with staff on all issues related to e-safety; Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place; Providing training and advice for staff; Receiving reports of e-safety incidents and creates a log of incidents to inform future e-safety developments; Co-ordinating and reviewing e-safety education programme in school.

Teaching & Support Staff
In addition to elements covered in the Staff Accessible Usage Policy (AUP), all teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They have read, understood and signed the school Staff Acceptable Usage Policy (AUP).
- E-safety issues are embedded in all aspects of the curriculum and other school activities.

- Pupils understand and follow the school's e-safety and acceptable usage policies
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended school activities
- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

Pupils (to an age appropriate level)

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Usage Policy, which they will be required to sign before being given access to school systems. Parents/carers will be required to read through and sign alongside their child's signature.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy also covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take opportunities to help parents understand these issues. Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Usage Policy.
- Accessing the school website in accordance with the relevant school Acceptable Usage Policy.

Community Users

Community Users who access school ICT systems/website/Learning Platform as part of the Extended School provision will be expected to sign a Volunteer User AUP (see Appendix 6) before being provided with access to school systems.

➔ 5. Cyberbullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class, and the issue will be addresses in assemblies

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, Advisory Panel and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

➔ 6. Education and Training

E-safety education will be provided in the following ways: A planned e-safety programme is provided as part of the school ethos and is regularly revisited in Information Technology and other lessons across the curriculum, this programme covers both the use of ICT and new technologies in school and outside of school.

Pupils are taught in lessons to be critically aware of the materials/content they access online and are guided to validate the accuracy of the information.

Pupils are helped to understand the need for the Pupil AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school.

Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.

Rules for the use of ICT systems and the Internet are posted in school

Staff act as good role models in their use of ICT, the Internet and mobile devices.

Acceptable Usage Policy (see Appendix 5/6)

Parents/carers will be required to read through and sign alongside their child's signature, helping to ensure their children understand the rules

Staff and regular visitors to the school have an AUP that they must read through and sign to indicate understanding of the rules.

Copyright

Pupils to be taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations- staff to monitor this.

Pupils are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.

If using a search engine for images – staff / children should open the selected image and go to its website to check for copyright.

Staff Training

The E-safety coordinator ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

A planned programme of e-safety training is available to all staff. An audit of the e-safety training needs of all staff will be carried out regularly.

All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy, Acceptable Usage and Child Protection Policies.

The E-Safety Coordinator/Head will receive regular updates through Local Authority and/or other information/training sessions and by reviewing guidance documents released.

Advisory Panel members are invited to take part in e-safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, e-safety, health and safety or child protection.

Email

Digital communications with pupils (e-mail, online chat) should be on a professional level and only carried out using official school systems (see staff guidance in Safeguarding and Child Protection Policy).

The school's email service should be accessed via the provided web-based interface by default (this is how it is set up for the laptops, school curriculum systems) or Outlook;

Under no circumstances should staff contact pupils, parents/carers or conduct any school business using personal email addresses.

School email is not to be used for personal use. Staff can use their own email in school (before, after school and during lunchtimes when not working with children) – but not for contact with parents/carers/pupils.

Mobile Phones

School mobile phones should be used to contact parents/carers/students, partnership schools and for any other school business.

Staff Staff are not permitted to use mobile phones or devices during working hours, unless on their break and not near children. Staff are not permitted to take photos of children on personal devices.

Pupils should adhere to the rules and guidelines set out in the Behaviour Policy regarding mobile phone use in school.

Social Networking Sites

Pupils will not be allowed on social networking sites at school; at home it is the parental responsibility, but parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites.

Staff should not access social networking sites on school equipment in school or at home.

Staff should access sites using personal equipment.

Staff users should not reveal names of staff, pupils, parents/carers or any other member of the school community on any social networking site or blog.

Pupils/Parents/carers should be aware the school will investigate misuse of social networking if it impacts on the well-being of other students or stakeholders.

If inappropriate comments are placed on social networking sites about the school or school staff then advice would be sought from the relevant agencies, including the police if necessary.

Pupils will be taught about e-safety on social networking sites as we accept some may use it outside of school.

Digital Images

The school record of parental permissions granted/not granted must be adhered to when taking images of our students.

Under no circumstances should images be taken using privately owned equipment without the express permission of the Head or the E-Safety coordinator.

Where permission is granted the images should be transferred to school storage systems (server or disc) and deleted from privately owned equipment at the earliest opportunity.

Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

Although many of the above points are preventative and safeguarding measures, it should be noted that the school will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information.

The school has an active website and twitter account which are used to inform, publicise school events and celebrate and share the achievement of pupils.

Removable Data Storage Devices

Only school provided removable media should be used.

All files downloaded from the Internet, received via e-mail or provided on removable media (e.g. CD, DVD, USB flash drive, memory cards etc.) must be checked for viruses using school provided anti-virus software before being run, opened or copied/moved on to local/network hard disks.

Pupils should not bring their own removable data storage devices into school unless asked to do so by a member of staff.

Websites

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.

Staff will preview any recommended sites before use.

"Open" searches (e.g. "find images/ information on…") are discouraged when working with younger students who may misinterpret information.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff. Parents will be advised to supervise any further research.

All users must observe copyright of materials published on the Internet.

Teachers will carry out a risk assessment regarding which pupils are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the pupils on the internet by the member of staff setting the task. All staff are aware that if they pass pupils working on the internet that they have a role in checking what is being viewed. Pupils are also aware that all internet use at school is tracked and logged.

The school only allows the E-Safety Coordinator, and the Head access to Internet logs.

Passwords - Staff - Passwords or encryption keys should not be recorded on paper or in an unprotected file. Passwords should be changed at least every 3 months.

Users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems.

Pupils

Should only let school staff know their in-school passwords.

Inform staff immediately if passwords are traced or forgotten. Staff are able to access the network to allow pupils to change passwords.

Use of Own Equipment

Privately owned ICT equipment should never be connected to the school's network without the specific permission of the Head or E-Safety coordinator.

Pupils should not bring in their own equipment unless asked to do so by a member of staff.

Use of School Equipment

No personally owned applications or software packages should be installed on to school ICT equipment;

Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted.

All should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

➔ 7. Filtering and Monitoring

The school will adhere to the Online Safety Policy at all times.

As part of a broad and balanced curriculum, all pupils will be made aware of online risks and taught how to stay safe online.

Through training, all staff members will be made aware of:

- Pupil attitudes and behaviours which may indicate they are at risk of potential harm online.
- The procedure to follow when they have a concern regarding a pupil's online behaviour.
- The procedures to follow if a pupil attempts to access content on school devices which is known to be banned or identified by the filtering systems.

The school will ensure that suitable filtering and monitoring systems are in place on ICT equipment to prevent children accessing inappropriate material, in accordance with the school's Data and Cyber-security Breach Prevention and Management Plan. The school will be working towards meeting the Advisory Panelnment's guidance on Meeting Digital and Technology Standards in Schools and Colleges. The school will ensure that filtering and monitoring systems do not cause over-blocking, which may cause unreasonable restrictions as to what people can be taught online. The DSL and Lead Advisory Panelnor for Safeguarding will monitor and regularly review these arrangements in line with KCSiE (paragraphs 124-148) requirements.

All staff should be clear on:
The expectations, applicable roles and responsibilities in relation to filtering and monitoring as part of their safeguarding training. For example, part of their role may be to monitor the content on pupils' screens. Staff must be aware and be able to articulate the software used by their school to filter and monitor content.

Staff must report safeguarding concerns if:

- They witness or suspect unsuitable material has been accessed.
- The pupils are able to access unsuitable material.
- They are teaching topics that could create unusual activity on the filtering logs.
- There is failure in the software or abuse of the system.
- There are perceived unreasonable restrictions that affect teaching and learning or administrative tasks.
- They notice abbreviations or misspellings that allow access to restricted materials.

School leaders should:

- Identify and assign roles and responsibilities to manage filtering and monitoring systems.
- Review filtering and monitoring provision at least annually.
- Block harmful and inappropriate content without unreasonably impacting teaching and learning.
- Have effective monitoring strategies in place that meet your safeguarding needs.

As part of the usual communication with parents, the school will reinforce the importance of pupils being safe online and inform parents that they will find it helpful to understand what systems the school uses to filter and monitor online use.

The school will use face to face opportunities to offer training to parents on how to keep their child safe online. The school and curriculum areas will make it clear to parents what their children are being asked to do online for school and the risks associated with that.

Reviewing online safety

School leaders will carry out an annual review of its approach to online safety, supported by an annual risk assessment that considers and reflects the risk faced by pupils. This will include an annual review of filtering and monitoring systems.

Filtering and monitoring systems will also be audited if there is:

- A serious breach of the school systems
- A change of provider

All use of the school's Internet access is logged and the logs are randomly but regularly monitored by the school's external provider. Whenever any inappropriate use is detected it will be followed up by the E-Safety Coordinator and the Head of Centre depending on the severity of the incident.

The E-Safety Coordinator and the Head of the Centre will record any breaches, suspected or actual, of the filtering systems. Any member of staff employed by the school who comes across an e-safety issue does not investigate any further but immediately reports it to the E-safety Coordinator and impounds the equipment. This is part of the school safeguarding protocol. (If the concern involves the E-Safety Coordinator then the member of staff should report the issue to the Head).

Incident Reporting

Any e-safety incidents must immediately be reported to the Head (if a member of staff) or the E-Safety Coordinator (if a pupil) who will investigate further following e-safety and safeguarding policies and guidance.

Responding to incidents of misuse

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

Listed in Appendix 3 are the responses that will be made to any apparent or actual incidents of misuse. If any apparent or actual, misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity or materials the flow chart should be consulted. Actions will be followed in accordance with policy, in particular the sections on reporting the incident to the police and the preservation of evidence.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a “clean” designated computer. 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 as follows (Appendix 3 for students and Appendix 4 for staff respectively).

➔ 8: Monitoring Arrangements

Monitoring arrangements The DSL logs behaviour and safeguarding issues related to online safety.

An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Computing Lead and Head of Centre. At every review, the policy will be shared with the Advisory Panelning board.

➔ Appendix 1: Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	STAFF & OTHER ADULTS				PUPILS & YOUNG PEOPLE			
Communication Technologies	Permitted	Permitted at certain times	Permitted for named staff	Not Permitted	Permitted	Permitted at certain times	Allowed with staff permission	Not permitted
Mobile phones May be brought to school	✓				✓			
Mobile phones used in lessons				✓				✓
Use of mobile phones in social time	✓				✓			
Taking photographs on mobile devices				✓				✓
Use of Ipads and other educational mobile devices		✓					✓	
Use of school email for personal emails				✓				✓
Social use of chat rooms/facilities				✓				✓
Use of social network sites			✓				✓	
Use of educational blogs	✓				✓			

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. 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 need to be aware that email communications may be monitored
- Users must immediately report to the nominated person (in accordance with the school policy) the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers (email, chat, Learning Platform 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 public chat/social networking programmes must not be used for these communications.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

➔ Appendix 2: Unsuitable/Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyberbullying 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.

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 school or outside school when using school equipment or systems.

The school policy restricts certain internet usage as follows. 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:

Please see table below:

Acceptable/Unacceptable Activities

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					✔
Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✔
Adult material that potentially breaches the Obscene Publications Act in the UK					✔
Criminally racist material in the UK					✔
Pornography					✔
Promotion of any kind of discrimination				✔	
Promotion of racial or religious hatred					✔
Threatening behaviour, including promotion of physical violence or mental harm					✔
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				✔	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				✔	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✔	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				✔	
Creating or propagating computer viruses or other harmful files				✔	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				✔	
On-line gaming (educational)		✔			
On-line gaming (non-educational)				✔	
On-line gaming				✔	

➔ Appendix 3: Incidents - Pupils

Incidents Involving pupils	Teacher to use school behaviour policy to deal with	Refer to pupil Head	Refer to police	Refer to technical support staff for action re security/filtering etc
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/		✔	✔	✔
On-line shopping / commerce	✔	✔		✔
File sharing	✔	✔		✔
Use of social networking sites	✔	✔		✔
Uploading to video broadcast e.g. Youtube	✔	✔		✔
Unauthorised use of non-educational sites during lessons	✔			✔
Unauthorised use of mobile phone/ digital camera/ other handheld device	✔			✔
Unauthorised use of social networking/ instant messaging/ personal email	✔	✔		✔
Unauthorised downloading or uploading of files		✔		✔
Allowing others to access school network by sharing username and passwords	✔	✔	✔	✔
Attempting to access or accessing the school network, using another student'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 instant message that is regarded as offensive, harassment or of a bullying nature		✔		✔
Continued infringements of the above, following previous warnings or sanctions		✔	Community Police Officer referral	✔
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		✔		✔

➔ Appendix 4: Incidents - Staff

Incidents involving members of staff	Refer to the Principal In event of breaches of policy by the Principal, refer to MSPRU	Refer to technical support staff for action re filtering, security etc	Referral to LADO Potential Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /inappropriate activities)	✔	✔	✔
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✔	✔	✔
Excessive or inappropriate personal use of the internet/social networking sites/ instant messaging/ 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	✔	✔	✔
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✔	✔	✔
Sending an email, text or instant 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 students/ 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	✔	✔	✔
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	✔	✔	✔

➔ Appendix 5: Acceptable Internet Use - Pupils

This document is a guide to pupils to be responsible and stay safe while using the Internet and other communication technologies. It clearly states what use of computer resources is acceptable and what is not. Irresponsible use may result in the loss of Internet or computer access, contact with parents or in the event of illegal activities contact with the police.

- I will only access the school network through my authorised username and password.
- I will not use the passwords of others.
- I will not use the school IT systems for personal or recreational use, for on-line gaming, gambling, internet shopping, file sharing or video broadcasting.
- I will not try to upload, download or access any materials which are illegal, inappropriate or which may cause harm and distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place.
- I will not try to install programmes on any school computer or alter computer settings.
- I will only use my personal hand held devices (e.g. mobile phone/ipad) in school at times that are permitted. This is commuting to and from school, or to contact parents after participation in an extra- curricular activity. When using my own devices I understand that I have to follow the rules set out in this document.
- I will carefully write email and other on-line messages making sure the language I use is not strong, aggressive or inappropriate and shows respect for others. I am responsible for the emails I send and the contacts I make.
- I will not open emails unless I know and trust the person/organisation who has sent them. For my own safety and that of others, I will not disclose personal information about myself or others when on-line.
- I will not arrange to meet 'on-line friends' unless I take an adult.
- I will not take, or distribute, images of anyone without their permission.
- I will only use chat and social networking sites with permission and at the times that are allowed.
- I will report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line. Where the material I research on the Internet is protected by copyright,
- I will not try to download copies, including music and video. I will only use the work of others found on the Internet in my own work with their permission.
- I will take care to check that information I find on the Internet is accurate and understand that some work found on the Internet can be untruthful or misleading.
- I will immediately report any damage or faults involving IT equipment, however this may have happened.

Signed Parent/Carer: ..... Date .....

Signed Pupil: ..... Date .....

➔ Appendix 6: Acceptable Internet Use - Staff

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The Internet and other digital information and communications are powerful tools, which open up new opportunities for everyone. These technologies can inspire discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users have an entitlement to safe Internet access at all times.

This policy is intended to ensure that:

- Staff and volunteers will be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.
- All IncludEd Learning ICT systems users are protected from accidental or deliberate misuse that could put the security of the systems or users at risk.
- Staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to improve learning opportunities for all and will, in return, expect staff and volunteers to agree to be responsible users.

Responsible Use Agreement

I understand that I must use ICT systems in a responsible way ensuring no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the use of ICT for enhancing learning and will ensure all learners receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with students.

For my professional and personal safety:

- I understand that the school will monitor my use of ICT systems, email and other digital communications.
- I understand the rules set out in this agreement also apply to the use of the school ICT systems (e.g. laptops, email, website) out of the school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username and password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material/incident I become aware of to the appropriate person (see policy charts).

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images.
- I will not use my personal equipment to record these images. I will not use chat and social networking sites in the school in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

IncludEd Learning, partner schools and the Local Authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held/external devices (Ipads/laptops/mobile phones/USB devices etc) in the school, I will follow the rules set out in this agreement, in the same way as if I was using the school's equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems. I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not (unless I have permission) make large downloads or uploads that might take up Internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Sharing Information Policy. Where personal data is transferred outside the secure LA network, it must be encrypted.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by policy to disclose such information.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the Internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of ICT equipment in school, but also applies to my use of school ICT systems and equipment out of the school and my use of personal equipment in the school or in situations related to my employment by IncludEd Learning.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, suspension, referral to the Advisory Panelnors, MSPRU/or the Local Authority and, in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use nornors Learning ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer

Name .....

Signed ..... Date .....

➔ Appendix 7: Online Safety Training Needs Self-Audit for Staff

Online Safety Training Needs Audit - Staff Self-Audit	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, Advisory Panelnors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	

Are there any areas of online safety in which you would like training/further training?	

➔ Appendix 8: Online Safety Incident Report Log

ONLINE SAFETY INCIDENT LOG

Online Safety Incident Report Log				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident
