Online Safety Policy

(Including Acceptable Use Agreement)

Policy title:	**Online Safety Policy**
Approved by:	**FGB**
Date approved:	**December 2025**

Policy review

Date of review	When / who carried out the review	Details of changes	Next steps

The online safety lead is the Headteacher

Using new learning technologies effectively and safely

This policy deals specifically with the educational and curriculum element of online safety. Guidance and procedure relating to infrastructure, networking and appropriate use of technology by staff are contained in the ICT security policy. Our online safety Policy has been written by the school, building on the Blackburn with Darwen policy guidance.

Writing and reviewing the online safety policy

The Online Safety Policy links to other policies including those for ICT, ICT Security, Anti-bullying, Cyber bullying and child protection.

- The Headteacher is the online safety lead
- The Headteacher is the DSL

Why the Internet and communication technology use is important

The safe use of technology is a part of the statutory curriculum and the internet a necessary tool for staff and pupils.

Ofsted guidance for schools 2013 recommends that all schools:

- Provide an age-related, comprehensive curriculum for online safety that enables pupils to become safe and responsible users of new technologies
- Audit the training needs of all staff and provide training to improve their knowledge of and expertise in the safe and appropriate use of new technologies
- Work closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and at school
- Use pupils' and families' views more often to develop online safety strategies.

School and community involvement in online safety policy and practice

At Ashworth Nursery School we believe that by involving representatives from all the school community in evaluating, formulating and reviewing online safety policy and practice, our children and staff will be the safest they possibly can be. Part of their role will be to contribute to online safety and practice and inform parents and peers of online safety issues on a regular basis.

Leadership of online safety

The responsibilities of the online safety lead are to:

- Maintain own knowledge of wider online safety and online safety leadership through training, seeking advice, and signing up to regular updates
- Regularly review the effectiveness of online safety policy and practice
- Ensure the computing curriculum is progressive and age appropriate and that there opportunities across the wider curriculum, including PSHE, to reinforce online safety messages
- Ensure all school staff receive online safety training annually and that a record of training is maintained
- Provide updates on online safety policy and practice to governors
- With the school's technical support, ensure that appropriate filtering and anti-virus software is in place
- Maintain reporting procedures for online safety incidents - This may be part of a wider reporting system, but should include access to inappropriate resources (intentional or otherwise), inappropriate use of school technology, online safety and cyberbullying disclosures. There should also be a record of how it

was dealt with and any consequences e.g. additional online safety input; discussion with parents restricting access etc.

- Provide or source online safety information and training for parents
- Ensure that appropriate acceptable use agreements are signed by pupils and parents and that permission for use of images and video is sought from parents (and pupils when appropriate)
- Ensure that the educational potential and possible online safety issues are investigated before using new technology.
- Annually review the school's online safety strategy, policy and practice

Online safety Education and Training

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience. Current guidance stipulates that it is not sufficient to just keep pupils safe in school. It is our responsibility therefore, to ensure they have opportunities to learn how to stay safe and deal with the risks associated with the internet and communication technology in the world around them. Keeping our children safe involves educating all members of our school's community, including governors, parents and all staff working in school.

Educating pupils

Our online safety curriculum

At Ashworth Nursery School we ensure that children have access to a progressive online safety curriculum.

Early Years Foundation Stage, Early Learning Goal

Children recognise that a range of technology is used in places such as homes and schools. They select and use technology for particular purposes.

In order to safely select and use technology we believe that children in the Foundation Stage need to be taught an age appropriate online safety curriculum.

The need to keep login details and other personal information private will be reinforced regularly when using the schools network and any other methods of communication agreed by the Headteacher.

Pupils will be taught how to evaluate Internet content appropriate to their age.

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught what Internet use is responsible and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation appropriate to their age group.
- Pupils will be taught about the dangers of radicalisation and extremism at an appropriate level for their age.

Educating parents

Children often seem more at home in the digital world than their parents. To ensure that children are the safest they possibly can be, we must educate parents about the risk of using the internet and communication technology for their children and the potential for their own use of technology to place themselves or their child at risk.

We ensure parents receive information and training by:

- Providing links to information and resources for parents on our school website
- Providing regular updates to parents through newsletters

- Inviting parents to online safety workshops
- Providing online safety information during events such as parents evenings
- Encouraging parents to act as role models when using technology
- The school will share with parents and children, our belief that:
- The unsupervised use of social network spaces intended for adults outside school is inappropriate for pupils of nursery/primary age.
- PEGI and BBFC ratings are good indicators of how appropriate the levels of violence, sexual content, bad language and the portrayal of drug taking and criminal acts are
- Family friendly filtering can help to keep children safe, however education and the opportunity to develop safe practice is essential for keeping children safe
- Pupils who use the internet and other communication technology may be at risk of being groomed or radicalised. It is important that parents understand that secrecy is a possible factor in both of these.
- What pupils do online now, can affect their future life.
- If a child is happy to tell a parent or carer when they are worried, they are the safest they can possibly be; therefore we encourage parents to nurture a sense of trust between them and their child when talking about using technology.

There are some excellent online tools for reporting concerns, such as the Report Abuse button which can be found on the https://www.thinkuknow.co.uk/ site and Childline http://www.childline.org.uk . Children are also encouraged to report their concerns via a member of staff or trusted adult.

Educating staff and the wider school community

- We ensure that all new staff receive online safety training as part of their induction
- All school staff have access to basic online safety training regularly
- The online safety lead and key members of the online safety group have access to a higher level of training, updates and information to ensure that have the skills and knowledge necessary to lead all areas of online safety.

Basic training

- Online safety issues for pupils
- Reporting procedures
- Guidance on appropriate use of communication technology by staff and pupils
- Guidance for staff on how to stay safe
- Expectations in terms of passwords and data security
- Expectations in terms of professional conduct including the use of social media
- Teaching pupils to minimise the screen if they see something that makes them feel uncomfortable.

Online safety training references and complements guidance in the Safer Working Practices document.

Keeping staff and pupils safe in school

All access to the internet is filtered by Light Speed. For further details on networking and filtering and how access to inappropriate sites can be monitored refer to the ICT Security Policy.

The school will work with the LA, and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it must be reported to the online safety

Lead who will inform the LA where appropriate so that they can take appropriate action. All users will be taught how to care for devices in terms of health and safety. This includes avoiding placing food or liquids near to electrical devices, carrying equipment and rules around charging and electrical sockets. The school internet access is designed expressly for pupil use and includes appropriate filtering. Sanctions for inappropriate use of the internet and communication technology follow sanctions set down in the behaviour policy. A record of any misuse is kept by the Headteacher.

At Ashworth Nursery School staff do not use their own personal devices/accounts to contact parents and pupils. Cameras/ iPad's are provided for recording school related activities. Images of children should not be stored on personal devices.

Acceptable use agreements

A home school agreement concerning access to the internet and communication technology will be signed by parents

- Class rules agreement linking to online safety and safer internet use
- Acceptable use agreement for school staff (see the ICT Security Policy)

Reporting online safety concerns

Children are encouraged to report their concerns via a member of staff. Where relevant, we also encourage the children to use national resources such as Child Line and CEOP.

Systems for reporting online safety concerns.

This should build on any systems for behaviour and safeguarding already in school. It should include:

- A record of online safety incidents is kept in the Online safety file in the Headteacher's office
- The nature of the incident and action taken are recorded with and any consequences e.g. additional online safety input; discussion with parents restricting access etc.. This includes access to inappropriate resources (intentional or otherwise), inappropriate use of school technology, online safety and cyberbullying disclosures.
- Published content - This will also be referenced in the in the ICT Security Policy
- Any information that can be accessed outside the school's intranet should be classed as published whether in electronic or paper format.
- Electronic communication sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- General contact details should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. (This may be through education and guidance, as directly reading everything is impractical)
- Where pupils publish work, there will be systems in place to check the content and pupils will be given clear guidelines about what can be published.

Publishing pupil's images and work

- Staff and pupils using digital cameras, video recorders or sound recorders will ensure that they inform others before recording them and always use equipment in a respectful manner. (In the Foundation Stage this may not be practical when capturing a child in the process of learning, however should be modelled as often as possible.)
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs or video of pupils are published.
- Where pupil's work is published the school will ensure that the child's identity is protected.
- Where school events are being publicised, care will be taken not to reveal information that may put children or staff at risk e.g. the date and location of a trip

Parents using still or video cameras at school

Guidance for taking photographs and video during school performances and assemblies can be found on the Information Commissioner's Office website: https://ico.org.uk/your-data-matters/schools/photos/

Managing emerging technologies

- The educational benefit of emerging technologies and any potential risks will be considered and shared with staff before they are used in school.

Protecting personal data

See the ICT Security Policy for guidance

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Responsible ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff that are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- In the Foundation Stage children will not be given access to the internet. Wi-Fi on children's IPAD's is switched off.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Blackburn with Darwen LA can accept liability for the material accessed, or any consequences of Internet access. Any inappropriate access whether intentional or unintentional will be reported to the e safety co-ordinator and to the LA where necessary.
- The school will audit ICT provision to establish if the online safety policy is adequate and that its implementation is effective.

Handling online safety complaints

- Complaints of Internet misuse will be dealt with by the Headteacher and where appropriate inform the LA.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure on request.

For further information, please see the ICT Security Policy

Introducing the online safety policy to pupils

- Online safety rules will be posted in all rooms where pupils may access the internet and discussed with the pupils at the start of each year. Where possible images and symbols will be used to help make them accessible to young children.

- Pupils will be informed that network and Internet use will be monitored and can be monitored and traced to the individual device or login.

Introducing the policy to parents

Parents' attention will be drawn to the School online safety Policy and practice:

- in newsletters,
- in the school brochure
- on the school website

Staff and the online safety policy

- All staff will be given the School Online Safety Policy and its importance explained.
- Staff should be aware that internet traffic may be monitored and traced to the individual device or login. Discretion and professional conduct is essential.
- The school may use monitoring software where this is available to ensure that inappropriate materials are not being stored or used on school equipment.

Please see the ICT Security and Acceptable User Policy for further information

Appendix 1 - Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's Acceptable Use Policy and Online Safety policy for further information and clarification.

- ICT equipment and software are the property of the school/Local Authority and I understand that it may be a criminal offence to use it for a purpose not permitted by its owner.
- I understand that I am responsible for my own use of new technologies, and will ensure that I use technology safely, responsibly and legally.
- I understand that school and personal ICT equipment may be used for private purposes out of school directed time only and that the use of school equipment may be monitored and should be in keeping with my professional status
- I understand that I must not use school ICT resources for personal financial gain, gambling, political purposes or advertising.
- I understand that my information systems and Internet use is subject to filtering and as such may be recorded.
- I will respect copyright and intellectual property rights. I will ensure that I have appropriate permissions before using or adapting work that may be the intellectual property of others and will acknowledge the source of all work that is not my own. **See appendix 5**
- I understand that it is my duty to protect my passwords and personal network login and should log off the network or lock the device before leaving it unattended.
- I will not install any software or hardware without permission.
- I understand my personal responsibility for safeguarding and protection of data and will comply with the data protection Act of 1998 and any other legal, statutory or contractual obligations that the school and LA inform me are relevant. **See appendix 5**
- I will familiarise myself with the public sector information classification framework. This national Protective Marking System classifies information in the following three levels of classification: unclassified, protect and restricted. **See appendix 4**
- I will report any known misuses of technology, including the unacceptable behaviours of others to the Head Teacher.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safeguarding to the designated senior person responsible for child protection.
- I will report any incidents of concern regarding suspected or actual failure of technical safeguards to the school Online Safety Lead.
- I will ensure that any electronic communications with pupils are appropriate to my professional role.
- I will ensure that all electronic communications are written in a professional manner and understand that they are potentially public property.
- I will promote online safety with pupils in my care and will help them to develop a responsible attitude to use ICT equipment and to the content they access or create.
- I understand that it is my duty to respect technical safeguards in place and will not attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services.
- I will take reasonable precautions to prevent damage to or loss of ICT equipment in my charge.

The school may exercise its right to record and monitor the use of the school's technology, including Internet access and email. The school will take the necessary action where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

- **I have read, understood and will abide by with the Information Systems Code of Conduct.**
- Signed:……Capitals……Date:……
- Accepted for school: ……Capitals:……Date:……

Appendix 2 Password security guidance

- Staff should use a strong password and keep it confidential. Never write your password down or store it in a computer system.
- Never reveal your passwords to anyone (includes colleagues, BT&IT Service Desk, Line Managers, family and friends)
- Never use the 'remember password' function.
- All users must prevent their username and password being used to gain unauthorised access by locking the workstation when it is not in use so that casual overlooking and unauthorised tampering is prevented.
- If you become aware, or suspect, that your password has become known to someone else, you must change it immediately and report your concern to the Online Safety Lead.
- Only use the user account to store data that is associated with the school.
- Users must not divulge their account passwords to others, must not permit others to use their accounts, and must not use accounts intended for the sole use of other individuals.
- Log off when leaving the room unattended.
- It is wise to save work before locking the workstation.
- Do not attempt to use your colleague's credentials.

A strong password contains a mixture of numbers, letters and punctuation

Appendix 3

ICT Asset Protocol

1. **Where any ICT Asset (any school or LA ICT equipment) is taken outside the site it shall be checked out by the relevant person (Headteacher) upon leaving the Site and checked in upon return.**
2. **Whilst any ICT Asset is outside the Site:**
    a. the person who checked it out shall be responsible for taking all reasonable precautions and care of it and for its safe return;
    b. it shall not be left unattended in any place or vehicle (whether locked or unlocked) other than the residence of the person who checked it out;
    c. during Core Hours ensure laptops & any other digital equipment is secured when rooms are empty for extended periods other than school break periods. Outside Core Hours, when not in use, teacher/administrator laptops must either be locked out of sight or taken home by the member of staff.
    d. it shall not be used where there is any material risk of damage from liquids, impact or otherwise;
    e. it shall not be lent or entrusted to any other person;
    f. Any alleged theft shall be reported to the police and a crime reference number obtained and until the number is obtained it shall be deemed to be a loss rather than a theft.

3. In using any ICT Asset:

a. users shall not attempt to modify or circumvent any antivirus or other security software;

b. users shall not save any data to the Asset that may cause damage or interference or instability to the Asset or any part of the Asset, including any firmware, operating system or other software;

c. Users shall comply with the Acceptable Use Policy when accessing the Wide Area Network.

d. The School shall ensure that any student or employee using ICT equipment out of school is aware of this protocol.

e. The school shall use reasonable endeavours to ensure that staff and students are informed of all further rules and procedures established from time to time by BwD (acting reasonably) to protect the security of ICT Assets.

f. Users with devices on long term loan are responsible for returning the device to school on a regular basis, to ensure updates are installed.

Appendix 4 - Information Classification

Information classification is a means of standardising the way information is assessed, marked and handled according to how confidential it is. The national Protective Marking System to classify information and has been introduced throughout the public sector as the standard framework to allow the safe and appropriate sharing and protection of information. Please familiarise yourself with the following 3 levels of classification from the Protective Marking System, which are referred to throughout this Policy:

Unclassified

UNCLASSIFIED is the lowest level of classification and covers all information which can safely be shared or is already publicly available.

Information is UNCLASSIFIED if:

• It is intentionally publicly available

• Disclosure would not adversely affect any individuals, external organisations or the school e.g. School literature, the school website, press releases, all items of public record.

Protect

PROTECT is the first level of sensitive information. Information should be classified as PROTECT if “compromise of information would be likely to affect individuals in an adverse manner.”

The PROTECT classification should be used where disclosure would:

• Be likely to affect an individual or a small number of individuals in an adverse manner

• Cause substantial distress to an individual

• Breach proper undertakings to maintain the confidence of information provided by third parties (for example, breach commercial confidence with a supplier to the school).

• Breach statutory restrictions on the disclosure of information.

E.g. documents/emails containing name, address, NI, DOB, commercial terms & conditions.

Most of the sensitive information which the school handles will be at the PROTECT level of classification.

Restricted

RESTRICTED is a higher level of classification than PROTECT and is used where “compromise of information would be likely to affect the national interests in an adverse manner”.

The RESTRICTED classification should be used where disclosure would:

• Put an individual at significant risk of harm or long-term distress

• Release personal information for 1000 or more individuals that is not in the public domain, even if the information is not likely to cause harm or distress (i.e. the release of a large amount of PROTECT classified data relating to individuals).

• Significantly undermine public confidence in the Council or other public body

• Cause widespread disruption to the work of the Council or other local public sector

Organisation

• Significantly impact the LA and Ashworth Nursery School's ability to discharge it's duties under the Civil Contingencies Act

The RESTRICTED classification will apply to a small amount of data which the school handles, primarily relating to highly sensitive information on individual students and staff. E.g. documents/emails containing, name, address, NI, DOB, Salary, Pension, Benefit details, investigations, fraud etc.

Appendix5

Data Protection and Other Relevant Legislation

The Legislation

5.1 Background

5.1.1 The responsibilities referred to in the previous sections recognise the requirements of the current legislation relating to the use of ICT systems, which comprise principally of:-

Data Protection Acts 1984, 1998 & 2018

Computer Misuse Act 1990;

Copyright, Designs and Patents Act 1988

5.1.2 It is important that all staff are aware that any infringement of the provisions of this legislation may result in disciplinary, civil and/or criminal action.

5.1.3 The general requirements arising from these acts are described below.

5.2 Data Protection Acts 1984, 1998 & 2018

The Data Protection Act exists to regulate the use of computerised information about living individuals and gives rights to individuals about whom personal data is recorded (Data Subjects). They may obtain personal data held about themselves, should be told about the use of personal data and can expect it to be accurate. The act places obligations on those who record and use personal data (Data Users). They must follow sound and proper practices, known as the Data Protection principles. Principle 7 requires that security is in place during the collection, use and storage of personal data.

Any requests to view personal data must be in line with the Data Protection and Access to Information procedures.

5.2.1 To be able to meet the requirements of the Act, the Headteacher is required to compile a census of data giving details and usage of all relevant personal data held on computer within the school and file a registration with the Data Protection Registrar. It is important that amendments are submitted where the scope of the system extends to new areas of operation. The 1998 Act is consistent with the principles established in the 1984 Act, but extends the regulation to certain manual records as well as computerised information. This shows you how to log on to the Information Commissioners Site and pay the necessary £35.00 for registration.

5.2.2 It is important that all users of personal data are aware of, and are reminded periodically of, the requirements of the act and, in particular, the limitations on the storage and disclosure of information.

5.2.3 Failure to comply with the provisions of the prevailing Act and any subsequent legislation and regulations relating to the use of personal data may result in prosecution by the Data Protection Registrar.

5.3 Computer Misuse Act 1990

5.3.1 Under the Computer Misuse Act 1990 the following are criminal offences, if undertaken intentionally:-

- Unauthorised access to a computer system or data;
- Unauthorised access preparatory to another criminal action;
- Unauthorised modification of a computer system or data.

5.3.2 All users must be given written notice that deliberate unauthorised use, alteration, or interference with a computer system or its software or data, whether proprietary or written 'in-house', will be regarded as a breach of school policy and may be treated as gross misconduct and that in some circumstances such a breach may also be a criminal offence.

5.4 Copyright, Designs and Patents Act 1988

5.4.1 The Copyright, Designs and Patents Act 1988 provides the legal basis for the protection of intellectual property which includes literary, dramatic, musical and artistic works. The definition of "literary work" covers computer programs and data.

5.4.2 If an organisation is using illegal copies of software the organisation may face not only a civil suit, but corporate officers and individual employees may have criminal liability. If liability is proven this could lead to an unlimited fine and up to ten years imprisonment per offence.

5.4.3 Where computer programs and data are obtained from an external source they remain the property of the originator. Our permission to use the programs or data will be governed by a formal agreement such as a contract or licence.

5.4.4 All copying of software is forbidden by the Act unless it is in accordance with the provisions of the Act and in compliance with the terms and conditions of the respective licence or contract.

5.4.5 All users must be given written notice that failure to comply with the provisions of the Act will be regarded as a breach of school policy and may be treated as gross misconduct and may also result in civil or criminal proceedings being taken.

5.4.6

The Regulation of Investigatory Powers Act 2000

The Act specifies that communications may be monitored and recorded for "a legitimate purpose" such as system and employee performance monitoring; detection and prevention of crime; detection of unauthorised use (including unauthorised use by employees; protecting against hackers and viruses; and ensuring the Council is complying with regulatory or self-regulatory practices or procedures relevant to the business.

Monitoring can only be carried out legally if the organization concerned has informed its staff that it is undertaking monitoring for these purposes. The provisions of the RIP Act have been taking into account in the formulation of Council policy relating to email and telephone use as detailed later in this document. Consistent with the LA and Ashworth Nursery School's policies for Misconduct and Workplace Harassment and Equal Opportunities, non-adherence to this policy may result in disciplinary action being taken by the Council that may result in dismissal and/or Civil or Criminal Court action.

Appendix 6

Unacceptable Use

This section does not provide a complete list of usage and behaviours that are considered unacceptable but it gives some examples of unacceptable use, in order to help all users of the ICT Service to make decisions on unclear areas.

The following activities will always be considered unacceptable use of Ashworth Nursery School's ICT environment by any user:

- Development, or deliberate release, of rogue code (i.e. viruses, Trojans, etc.).
- Interference with the work of other users (e.g. altering or copying their work).
- Grooming.
- Hacking, probing, scanning or testing the weaknesses of a system systems within Ashworth Nursery School's ICT environment, or on the Internet. Unauthorised access to systems. Violating or attempting to violate the security of the network.
- Actions that bring the school, or Ashworth Nursery School's ICT environment, into disrepute, or that are likely to do so.
- Deliberately wasting resources (e.g. unnecessary copying or emailing or very large files).
- Use of the environment for personal financial gain.
- Any illegal activity, including breach of copyright.
- Attempting to log on using another person's username and password.
- Making your username and password known to any unauthorised person.
- Creating or storing offensive, intimidating, insulting or harassing material on the school network.
- Accessing data not intended for you to access.
- Attempting to bypass filtering, or to access inappropriate or illegal material – such attempts will be reported to the school authority.
- Leaving your workstation logged in while unattended.
- Connecting additional devices to data points on the Schools network
- Attempting to interfere with services to any user, host or network.
- Taking any action in order to obtain services to which you are not entitled.
- Conducting any unlawful or illegal activity.
- Using the services to create, transmit, distribute or store content that invades the privacy or other personal rights of others.
- Assisting, encouraging or permitting any persons in engaging in any of the activities described in this section.
- Sending email messages which result in complaints from the recipient or from the recipient's email provider, or which result in blacklisting of the sender's email address or mail server.
- Sending email or messages which are excessive and/or intended to harass or annoy others.
- Sending, or attempting to send, spam of any kind from third-party networks using a return email address that is hosted on the Schools mail servers, or referencing an email address hosted on the Schools mail systems.
- Failing to observe intellectual property
- Keeping, accessing or transmitting confidential data about other students.
- Producing documents, creating blogs, creating or engaging with social networking sites or creating/sending emails that contain obscene, offensive, unlawful, intimidating, defamatory, harassing,

abusive, fraudulent, or otherwise objectionable content as reasonably determined by the school or authority.

- Causing technical disturbances to the ICT systems by introducing viruses of any kind.
- Any use that interferes with, or prevents, another user's permitted use of the environment.
- Unauthorised modification or reconfiguration of Ashworth Nursery School's ICT systems.
- Using managed service email or messaging systems to engage in inappropriate or non-professional communications between staff and students.
- Any uses of school ICT equipment of personal equipment connected to the network, intended to bully or harass others.