Newfield
Inspire | Support | Achieve | Together

ICT Acceptable Use Policy

1 Contents

'Newfield School is committed to safeguarding and protecting the welfare of children and vulnerable adults as it's number one priority. This commitment to robust recruitment, selection and induction procedure is shared by all staff and volunteers of Newfield School.'

2 Introduction

This policy outlines the secure use of computer equipment on the Blackburn with Darwen Schools Network (BWD) and Newfield Schools ICT network.

Newfield School, BWD are committed to protecting employees, partners and students from illegal or damaging actions by individuals, either knowingly or unknowingly. Newfield School and the local authority (BWD) will take appropriate steps to protect the school ICT equipment and environment from threats, including but not limited to unauthorised access, computer viruses, violation of privacy and interruption to service.

1.1 Purpose

The purpose of this policy is to:

- Define the acceptable use of Newfield School IT equipment and environment
- Ensure all use of IT equipment and environment is legal, ethical, and consistent with the aims, values and objectives of the LA and Newfield School.
- Inform all users of their personal responsibilities when using Newfield School IT equipment and environment.
- To protect Newfield School IT environment information assets and services from all threats whether internal or external.
- To ensure that those who use the School IT environment are aware of the requirements of IT Security and Acceptable Use.
- To ensure that those who use the environment are aware of their roles and responsibilities in applying, enforcing and complying with IT Security and Acceptable Use.

1.2 Objectives

The objectives of this policy are:

a) To ensure that equipment, data, staff and pupils are adequately protected on a cost-effective basis against any action that could adversely affect the school.

b) To ensure that users are aware of and fully comply with all relevant legislation and guidance around ICT security and safe and acceptable use of ICT.

c) to create and maintain within the school a level of awareness of the need for ICT security to be an integral part of the day to day operation so that all staff understand the need for ICT security and their own responsibilities in this respect.

1.3 Definitions

For the purposes of this document the terms 'ICT' (or 'ICT system') 'ICT environment, 'ICT data' and 'ICT user' are defined as follows:-

- 'ICT' (or 'ICT system') means any device for automatic storing and processing of data and includes servers, minicomputer, microcomputer, personal computer (whether hand-held laptop, portable, stand-alone, network or attached to a server network), workstation, word-processing system, desktop publishing system, office automation system, messaging system, any other similar device and peripherals for these devices.

- ICT Environment means any virtual, online or networked resource or facility available through the School.

- 'ICT data' means any information stored and processed by ICT and includes programs, text, pictures and sound (see Appendices 4 and 5)

- 'ICT user' applies to any Authority employee, member of school staff, pupil or other authorised person who uses the school ICT systems and/or data.

1.4 Scope

This policy applies to all users of Blackburn with Darwen and Newfield school equipment and environment and must be adhered to at all times. It also sets expectations for the appropriate, legal and safe use of all equipment in school, including legacy equipment and devices belonging to staff and pupils.
It also covers:

- All equipment that is owned or leased by Newfield School.
- Guest devices authorised by Newfield School, to connect to services.
- All employees, contractors and temporary staff, outsource agents and other workers at Newfield School, who are responsible for the administration and management of the Newfield School ICT environment.
- All those who use the Newfield School ICT services including both students and staff.

1.5 Other Related Policies

The contents of the related policies should be maintained in conjunction with the ICT Acceptable Use Policy. (See Appendix 7 for related policies)

1.6 Expectations

The contents of this policy should be used as a basis for each school to create and distribute an acceptable use agreement. The appropriate AUA should be signed by all staff and students where possible. A signed AUA form should be returned before a user is permitted access to Newfield ICT services. Signed AUAs should be stored safely for future reference by the distributing school.
All school staff have a responsibility to familiarise themselves with this policy before using the Newfield IT equipment and environment. All users must read, understand and sign to verify they have read and accepted this policy before using Newfield IT equipment and environment. (See Appendix 1).

Any user found to have breached the terms of this policy, may be subject to the Newfield School disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

2. Compliance with Policy

The Newfield ICT environment is provided to support learning within BWD education system. All those accessing the Newfield School ICT environment, whether students, staff, or those managing it, will comply with all current legislation in England, in addition to any requirements placed on them by this security policy. This includes compliance with legislation designed to protect personal information, legislation covering software and similar intellectual property licensed from third parties, and cooperation with Law Enforcement agencies.

2.1 Compliance with Policy for all users

The primary usage will be to support school educational and pastoral activities. Full compliance with the acceptable use policies and policy standards is expected, including:

- Compliance with and adoption of the agreed password standards (Appendix 2)
- Adoption of safe practices to ensure the integrity of the ICT environment, password security and data security.
- Compliance with the appropriate reporting mechanisms should they suspect an account has been compromised, ICT security breached or safeguarding issues arise.

The Newfield IT Systems are provided primarily for the purpose of conducting and supporting learning and teaching activities; however personal usage is permitted as long as this does not:

- Take place during lesson time or otherwise interfere with the user's professional role.
- Bring the local authority or Newfield School communities into disrepute
- All Newfield IT Systems users should be aware that usage may be monitored and/or recorded; misuse of the Newfield IT Systems may lead to disciplinary action.
- In such situations, the Authority will be the arbiter of whether or not the use was reasonable in the circumstances, with support from BWD ICT Services Department.

2.2 Compliance with Policy for school staff

In general, the acceptable use standard for school staff is the same as for students except:

- It is acceptable for a member of the school staff to access and use one of their students' personal accounts, in order to assist the student in using the Newfield ICT environment.
- In some circumstances (e.g. where work has been completed but not submitted and a student is unavailable) it is acceptable for a member of the school staff to access a student's files.
- A student's work may be altered by an appropriate member of the school staff, if this is done visibly, and for the purpose of marking and correcting the work.
- Members of the school staff should not alter a student's work in such a way that the corrected file appears to be the student's own work.
- Members of the school staff should not use any other users ICT Service user account login for work or personal matters.

2.3 Compliance with Policy for temporary users

All temporary users will be required to:

- Sign the acceptable use agreement and agree to abide by the requirements set out in this policy.
- Sign the relevant E-Safety AUA and agree to abide by the E-Safety policy.

2.4 Compliance with Policy for Operations Staff and Authority Staff

Newfield ICT operations staff and Authority staff may have access to other users' information and files within the School ICT environment. This information will only be accessed for operational purposes. It must never be copied outside the School ICT environment. Inappropriate access to, or misuse of, personal information within the School ICT environment will be considered a disciplinary offence

3 ICT Security

A number of different groups have responsibility within Newfield School ICT for aspects of IT Security.

3.1 Governing Body Responsibilities

The governing body has ultimate corporate responsibility for ensuring that the school complies with the legislative requirements relating to the use of ICT systems and for disseminating policy on ICT security and other ICT related matters. In practice, the day-to-day responsibility for implementing these legislative requirements rests with the Head teacher.

3.2 Head teacher Responsibilities

The Head teacher is responsible for ensuring that the legislative requirements relating to the use of ICT systems are met and that the school AUP/ICT Security Policy is adopted and maintained by the school. He/she is also responsible for ensuring that any special ICT security measures relating to the school ICT facilities are applied and documented as an integral part of the Policy.

The Head teacher, in accordance with the School Financial Regulations, shall ensure that an inventory of all ICT equipment (however financed) is maintained and all items accounted for at least annually.

In practice, the day to day functions may be delegated to Newfield ICT Services Department, who will keep an inventory of equipment within their remit and the School Finance Manager who maintains the Asset Register.

The Head teacher is also responsible for ensuring that the requirements of the Data Protection Act 1998 are complied with fully by the school. This is represented by an on-going responsibility for ensuring that the:-

- registrations under the Data Protection Act are up-to-date and cover all uses being made of personal data.
- Registrations are observed with the school.
- School has a current Data Protection Policy, clearly defining how they assess and record levels of protection data.
- School is compliant with General Data Protection Regulation (GDPR 2018)

In addition, the Head teacher is responsible for ensuring that users of systems and data are familiar with the relevant aspects of the Policy that the appropriate controls are in place for staff to comply with the Policy. The Head teacher or Chair of Governors should ensure that details of any suspected or actual breach are recorded and made available to Internal Audit upon request. The Head teacher or Chair of Governors must advise Internal Audit of any suspected or actual breach of ICT security pertaining to financial irregularity. The reporting of any breaches in GDPR regulations within 72 hours of a breach occurring.

3.3 Internal Audit responsibilities

The Internal Audit Section of Blackburn with Darwen is responsible for checking periodically that the measures prescribed in each school approved ICT Security Policy/AUP is complied with, and for investigating any suspected or actual breaches of ICT security.

Specialist advice and information on ICT security may be obtained from the Education ICT Group, who will liaise with Internal Audit on such matters.

3.4 School Responsibilities

The governing body and Head teacher are ultimately responsible for all school responsibilities.

The school is responsible for:

- Ensuring appropriate arrangements are applied for the removal of any ICT equipment from its normal location. These arrangements should take into

consideration the risks associated with the removal and the impact these risks might have.

- Giving adequate consideration to the physical security of rooms containing ICT equipment (including associated cabling). As far as practicable, only authorised persons should be allowed access to the school server or servers that provide access to data.
- Defining and documenting the requisite level of protection for data and documents according to the information classification system.
- Defining and documenting appropriate levels of access to the network and associated resources including the Information Management System (SIMs).
- Ensuring staff with higher levels of access sign any additional documentation as required
- Ensuring the Ethical and safe disposal of decommissioned equipment.
- Ensuring the Integrity of data, both during repair of faulty equipment and the disposal of assets.

3.5 User accounts

Access to the environment will be by individual user accounts for staff and group accounts for pupils. All users will be required to comply with minimum password standards appropriate to the user group.

- It is the responsibility of the school to ensure that enabled user accounts are available only for current staff and students and that the IT Department are informed of accounts to be disabled or removed.

• The user account of anyone who is under investigation for inappropriate use of the system must be disabled promptly.

• Newfield IT Department may generate test accounts for the purpose of technical systems monitoring; however no other user accounts should be created for fictitious staff or students. 'Generic' or group usernames (i.e. accounts that could be used by more than one person) will only be created in special circumstances and must be agreed beforehand by the Head teacher and access restricted as appropriate.

Access to another users data may be given in exceptional circumstances. Should this be required users should seek advice from the Head teacher and IT Department.

3.6 Equipment sitting

Reasonable care must be taken in the sitting of computer screens, keyboards, printers or other similar devices. Wherever possible, and depending upon the sensitivity of the data, users should observe the following precautions:-

- Devices should be positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to view the information. Specific consideration should be given to the sitting of devices on which confidential or sensitive information is processed or retrieved;

- Users should avoid leaving computers logged-on when unattended if unauthorised access to the data held can be gained. Clear written instructions to this effect should be given to users;

- A 'clear desk policy', i.e. hard copies of sensitive data are not left unattended on desks.

The same rules apply to official equipment in use at a user's home.

3.7 All users responsibilities

All users will sign a user agreement before using Newfield ICT equipment. They will also receive induction training at an appropriate level to ensure they are able to use the system confidently and safely. Where users have access to sensitive data, they will receive training on data security before accessing data at an appropriate level on the network.

All users of the school ICT systems and data must comply with the requirements of this Acceptable Use Policy, which are summarised in *Acceptable Use Agreement*' attached as Appendix 1.

All users are responsible for:

- The use of their unique logon details (username and password) and email address and for all content that is transmitted received and stored by their user account.
- It is of utmost importance that the password and access to users accounts remain protected at all times. See guidance document in Appendix 2.
- Reporting concerns over password security immediately
- Users are responsible for notifying the Head teacher or Designated Senior Persons in school of any suspected or actual breach of ICT security. Where the level of breach requires it, the Head teacher should inform Internal Audit.
- Looking after all computer equipment, ensuring they leave PCs and peripherals in the condition in which they were found.
- Ensuring any mobile devices used in school are, when not in use, switched off fully, connected for charging and stored in a secure place.
- Endeavouring to protect Newfield equipment and network against Viruses, Malware, Zero Data Attacks and other forms of software based attacks
- Reporting any inappropriate use of Newfield ICT services (see section 7).

- Following the ICT Asset Protocol when taking any school ICT equipment off the schools premises.
- Users should report any incidents, either perceived or real, to the Head teacher or Designated Senior Person at the school. The Head teacher and Designated Senior Persons are responsible for escalating such incidents to the Newfield School IT Department who will in turn investigate the incident.

Users should not make any attempt to disable or reconfigure any IT security measures or software on Newfield equipment or environment, including Anti-virus software or seek to bypass any monitoring, filtering or security measures that are in place.

Users are responsible for ensuring all data requiring backup is stored on Newfield network and not saved on individual computers.

3.8 Staff users additional responsibilities

Staff users are responsible for;

- Protecting access to their account, and for maintaining the appropriate confidentiality of their data.
- Ensuring privacy of pupil data
- Storing data appropriately
- Ensuring pupils in their care are reminded regularly of expectations around appropriate use of Newfield ICT environment, ICT security and E-Safety
- Returning portable equipment signed out to them for updates when requested to do so.

3.9 Newfield IT Department

Newfield School IT employees have responsibility for:
Ensuring all data held on the network is backed up.

- The configuration, operation and on-site support of all Newfield School ICT services. Within the context of security they are responsible for bringing any security incidents, either perceived or actual, to the attention of the Head teacher.
- Day to day management of the school ICT equipment, systems and data including responsibility for controlling access to these assets.
- Administering the practical aspects of ICT protection and ensure that various functions are performed, such as maintaining the integrity of the data, producing

the requisite back-up copies of data and protecting the physical access to systems and data.
- Ethical and safe disposal of decommissioned equipment covered by the school
- Integrity of data during both repair of faulty and disposal of equipment.
- Measures to guard against unauthorised access to data, such as ensuring that all data is held in a secure location.
- Ensuring approved security patches and service packs are in place on all devices.

3.10 Business Continuity

Business Continuity is an integral part of managing records both under Data Protection Act 1998 and Freedom of Information Act 2000. It is also important to ensure that if a major incident does occur then Newfield School can continue to operate and ensure that all the required information is available.

The two types of major incident that may affect Business Continuity are:
- Major Computer failure
- Environmental incidents e.g. fire

Regular backups of all information are undertaken by IT Department using VEEAM and Data Protection Manager Back Up systems. Information is stored on and off site via Tape Backup. In the event of any incident all information can be retrieved and restored.

Paper records are stored in locked metal filing cabinets or cupboards which would ensure that most, if not all records could be salvaged.

(See also Section 3.9)

4 Online communication and use of the web to download/ upload information

4.1 Provision

<u>Internet access</u>

The provision of the Internet access is owned by the Council and all access is, recorded and logged. This supports the performance of internal investigations and the management of systems as well as helping to ensure compliance in accordance with the Regulation of Investigatory Powers Act 2000.

Users browse the Internet through a filtered service that is designed to reduce the risk of access to inappropriate material. Nevertheless this filtering cannot be 100%

effective, and users should be aware of the possibility of access to inappropriate material and know what to do if such material is displayed (See the school's E-safety Policy). Please note that this service is managed by BWD with Tier access control at school level. Where a user's job role requires them to access inappropriate or restricted sites, approval must be obtained from the head teacher prior to access.

Email

All users will be provided with individual Office 365 email accounts and are able to use these for communication with other students and staff, both within their own school and with other schools. When the facility is available, this system will be managed by the school to ensure access is appropriate to the school requirements.

Email to and from the Internet is permitted, but students should receive E-Safety education before using the system (Please see our E-Safety Policy). It should also be noted that email and attachments may need to be disclosed under the Data Protection Act 1998 (see Appendix 2) and the Freedom of Information Act 2000.

4.2 Guidance on use

All use of electronic forms of communication or use of the web to share, access download or publish information, should:

- Ensure that personal and financial information is safeguarded, including personal contact details.
- Ensure the security of the ICT network by maintaining up to date virus protection and following links downloading files from reliable sources only.
- Always use their 'newfield.blackburn.sch.uk' email addresses when sending, receiving or forwarding emails containing RESTRICTED information and encrypt when necessary.
- Access news groups, bulleted boards and other similar communication groups for educational purposes or those relating specifically to their professional role only.
- Use social networking sites, real time chat, discussion forums, online games and other similar web resources only when expressly permitted to do so for educational purposes, or as part of a member of staff's professional role.
- Only publish information they have permission to use from the school and individuals
- Abide by copyright laws and licensing constraints regarding the use of software and electronic media.

Boundaries around publishing publicly accessible information and resources should be agreed on a school basis, with staff given appropriate permissions and clear guidelines as to acceptable content.

Use of electronic forms of communication or web access to share, download or publish information, for the following purposes is not permitted and may result in disciplinary and legal action where necessary.

- Sending, receiving, accessing or downloading obscene, racist, or insulting language, images, video or other media.
- Sending, receiving, accessing or downloading content in any form, containing provocative, suggestive or discriminatory language.
- Engaging in activities that bully, harass, mislead others or cause distress to groups or individuals.
- Accessing sites that are violent, hateful and discriminatory, promote hacking, or encourage gambling.
- Revealing information of a personal or private nature, or information that may lead to identification of an individual.
- Sending SPAM
- Downloading, uploading sharing or copying any content of copyrighted material, unless permission has been sought and given by the owner of the copyright (Please note breaching this is a criminal act and may lead to personal prosecution).
- Forwarding emails or information containing personal, confidential or sensitive information (therefore classified as PROTECT or RESTRICTED information - see Information Classifications Section) from the Blackburn.gov to any personal email addresses including the employee's own personal email.
- Sending or forwarding emails containing RESTRICTED information to recipients outside the school who do not have 'blackburn.gov' email accounts. This should be done through your standard school email address with appropriate encryption. Contact the BT&IT
- Using the LA and Newfield School IT Systems to support private business or money making activities.

Any use that may potentially bring the users, the school and or the local authority into disrepute. (where a user is unsure whether a particular use is acceptable, it is the users responsibility to consult their Line Manager who will seek further advice as necessary.

5 Portable Devices and External Connections

Facilities are in place to allow the transfer of information into and out of the Newfield School ICT environment by removable media (e.g. CD, pen drive, flash memory card, removable hard drive etc). Automatic anti-virus and security tools are in operation to scan material during such transfers. If you are unsure please contact the IT Department.

5.1 External Network Connections

The Authority Representative and the School ICT Services Manager will work with school under an Operational Change Control to explore requests for any external connections to access the School ICT Network.

5.2 Removable Media and Mobile Devices

Securing PROTECTED or RESTRICTED data is of paramount importance – particularly in relation to the LA and Newfield School the need to protect data in line with the requirements of the Data Protection Act1998. When using portable devices and removable media:

- Permission should be sought and an assessment of risks, especially relating to information assurance, should be carried out before taking mobile devices out of the school site. (Appendix3)
- Users should sign to acknowledge receipt of loan devices.

Users should not engage in the following activities when using portable devices and removable media:

- Any action designed to circumvent anti-virus and ICT security measures when connecting school equipment to private networks, or when accessing school services/ resources through private networks.
- Storage of PROTECT or RESTRICTED material. (See Appendix 4)
- Storing any data on removable media or mobile devices once it has been transferred / used.

5.3 Devices connected to the Newfield IT network

Any device connected to the Newfield IT network must comply with the following rules:

- All network servers and desktops must have adequate, up-to-date anti-virus protection or end-point security tools with automatic updates.
- Up-to-date security patches and service packs must be in place on all devices.
- Authority must be sought from the IT Department and team leader to perform a risk assessment before guest devices can be connected to the Newfield network/environment.

Any loss or theft of removable media or portable devices must be reported immediately to the IT Department and to the School Finance Manager.

6 Storage and installation of Software, resources and data

The use and storing of information by the (LA) School is controlled by certain Acts of Parliament. There are obligations for the School and members of its community that need to be followed. (see Appendix...)

The owner has the legal title to the property. In this respect, all software, data and associated documentation produced in connection with the work of the school are the legal property of the Local Authority, which will normally hold it for the benefit of Newfield School.

Exceptions to this will be allowed for software and documentation produced by individual Teachers when agreed in writing by the Head teacher.

We also use software and data that are the legal property of external organisations and which are acquired and used under contract or licence.

6.1 Licenses

Software license compliance requires all software used within the School is legally licensed, in accordance with the Copyright, Designs and Patents Act 1998.

It is the responsibility of the school to ensure that all software on the school IT network is appropriately licensed.

The school is responsible for compiling and maintaining an inventory of all software held by the School and for checking it at least annually to ensure that software licences accord with installations.

To ensure the School is compliant the following rules must be adhered to:

- All software must be purchased with a licence appropriate to its intended use.
- All software to be installed on Newfield IT equipment must be tested by the IT Department prior to installation. This includes all Commercial, Shareware, Freeware, and Public Domain Software.
- The (LA) School expressly prohibits the illegal duplication of software.
- Copying, downloading and storing of copyrighted material (such as music, and photographs from magazines) that is not waivered for educational use on Newfield IT equipment and is strictly prohibited.
- It is the responsibility of the school to ensure that software added to all devices and desktops on the network, including guest devices, is appropriately licensed.

Please be aware that failure to follow this policy could lead to criminal prosecution.

6.2 Data Ownership

Data within the Newfield School ICT environment will be owned by a number of different individuals and organisations.
The Authority will have the final decision on the ownership of any particular item. All data will be handled in a manner appropriate to its sensitivity.

Legal Responsibility

Blackburn with Darwen Borough Council collects, holds and uses data about people and organisations with whom it deals with in order to conduct its business.
Blackburn with Darwen Borough Council fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998, and other relevant information security legislation.
Data protection and privacy must be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. Key records must be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.
(See Appendix 5 and the school's Data Protection Policy).

6.3 Protection of Data

The Authority and Newfield School will take appropriate steps to prevent, loss or incident, whether accidental or malicious, including error, fraud, damage and disruption

to computing or communications facilities. Those operating procedures laid down in the project agreement will be adhered to in order to minimise the risk of loss of data within the Newfield School ICT environment.

7 Dealing with incidents of unacceptable or inappropriate use.

7.1 Systems and Security Monitoring

All users should be aware that in order to provide a secure environment the following detective security controls are in place:

- Email systems are filtered and recorded through Office 365
- Web usage is actively filtered and recorded
- System usage is recorded
- System files, etc may be accessed to ensure confidentiality integrity and availability.
- All ICT services are monitored and audited, including using automated alerting systems. Logs will be retrieved after an incident has occurred in consultation with BwD.
- All users are responsible for security of Newfield ICT systems, including appropriate use of resources such as email and the internet.
- Parents and carers will be informed of the expectations and responsibilities of their child when using Newfield ICT remote services and encouraged to support their child in fulfilling the expectations.
- Any school user data retained by filtering systems will not be released unless authorisation has been given by the Head teacher or an appointed member of staff.
- Checks will be carried out to identify violations such as placing rogue equipment or software on the network or systems.

7.2 Reporting

Any inappropriate or unacceptable use of the school ICT equipment or personal devices during school time should be reported to the appropriate organisation as follows:

- The Head Teacher or Designated Senior Lead.

7.3 Consequences

Newfield School and the local authority reserves the right to suspend or terminate an account if a security breach is encountered. The unacceptable use will be investigated as a security incident and the school will be advised of the activities carried out by the user. The school will decide on the appropriate disciplinary action.

Any violations of this security policy should be brought to the attention of the relevant authority that will work with the suitable individuals to rectify the problem.
Violation of this security policy by a Newfield School IT employee or a member of school staff may lead to disciplinary proceedings and/or legal proceedings against that individual by the appropriate employing authority. Intentional or persistent violation of this security standard by contract staff, or by staff of third parties in a contractual relationship with Newfield School, will be treated as a breach of the appropriate contract. Where a student is involved in intentional persistent violation of this policy, appropriate action will be taken by the Head teacher.

7.4 Incident Response Investigations

The school ICT Services Manager and an authority representative should instigate an investigation of any security incident, with a view to determining the appropriate actions to take as a result of the incident.

The investigation should, wherever possible, determine the extent of an incident, the impact of the incident, and the source of the incident. It may not always be possible to complete such investigations, but an attempt should be made to get far enough to make a reasonable recommendation as to actions that should be taken as a result of the incident. Where a security incident affects Newfield school the IT Manager should exchange appropriate information with the Authority, in order to coordinate the resulting actions. This notification should take place at the earliest appropriate time.

It is particularly important that all security and E-Safety incidents are logged and that a detailed record is kept of the investigation and resultant actions. **The ICT Services Manager is responsible for this log**, even though other people will carry out specific parts of the investigation and resultant actions. Reports should be submitted to the Authority for review or further investigation.
All security incident reports and logs must remain confidential and only authorised personnel will be permitted to view this material.
The local law enforcement agency will be contacted if the severity of a security breach necessitates this course of action under advice and guidance from the Head teacher.

Investigations are normally conducted for all security incidents including but not limited to the following:

- Unauthorised access or an attempt to access a resource or other users account without approval.

- Unauthorised modification to systems whether successful or unsuccessful.
- Unauthorised disclosure of school information.
- Deliberate or unintentional hacking attempts such as Denial of Service attacks, etc.
- Rogue software or hardware appearing on the Newfield School network.

8 Policy review

This policy will be reviewed by Newfield School annually. Due to the rapidly changing nature of technology, this policy may be updated more regularly as a result of advice from the LA. Any changes should be shared with staff at the earliest possible opportunity.

Appendix 1 – IT Acceptable User Agreement

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 e-safety policy for further information and clarification.

IT Acceptable User Agreement (AUA)

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 e-safety policy for further information and clarification.

- ICT equipment and software are the property of the school and I understand that it may be a criminal offence to use it for a purpose not permitted by its owner.
- I will ensure that my use of technology will always be compatible with my professional role and equipment may be used for private purposes out of school directed time only and that the use of school equipment may be monitored.
- I understand that I must not use school ICT resources for personal financial gain, gambling, political purposes, purchases or advertising.
- I understand that the school will monitor my information systems and Internet use to ensure policy compliance.
- 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
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safeguarding and any suspected or actual failure of technical safeguards to the school e-Safety Coordinator, or the designated senior person responsible for child protection
- I will ensure that any electronic communications with pupils are appropriate to my professional role and are written in a professional manner and understand that they are potentially public property.
- I understand that as part of a pupil's assessment of needs, additional support from staff, specialist access equipment or specific resources may be identified. If this is the case, I will be required to act as pupil advocate. I agree that I will take

responsibility for their login details and treat them with the same respect for privacy and confidentiality as my own login details.

- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I understand that I have a duty to promote the child's agenda when using technology. Taking direction from the child themselves wherever possible.
- I understand that electronic communication between children and adults, should take place within clear and explicit professional boundaries.
- I will not share any personal information with a child or young person or request or respond to, any personal information from the child/young person, other than that which might be appropriate as part of my professional role.
- 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 all reasonable precautions to prevent damage to or loss of ICT equipment in my charge.
- The school will take the necessary action where it believes unauthorised use of the school's information system may be taking place.

ICT Acceptable Use Policy

Failure to comply with the guidelines in this policy could result in the implementation of the school's Disciplinary Policy

This consent form must be agreed with reference to the 'Guidance for Safer Working Practice', Newfield E Learning and Child Protection policies.

I have read, understood and will abide by with the IT Acceptable Use Policy and Agreement.

Print Name:

Signed:

Date:

Appendix 2 - Password Security Guidance

Password Policy - Strong

Attribute	Strong
Password History Length	10
Password Complexity Status	TRUE
Minimum Password Length	7 Characters
Minimum Password Age	0 days
Maximum Password Age	60 days
Lockout Threshold	5 invalid logon attempts
Lockout Observation Window	30 minutes
Lockout Duration	30 minutes

Composition
This policy would require the user to have at least a 7 digit password made up of a combination of character types. Passwords cannot be the same as the previous 10 passwords.
The password will expire after 60 days.
The account will lockout after 5 invalid attempts, but will automatically unlock after 30 minutes.

Security
This is the most difficult to use but in terms of security this policy is the strongest as the risk for unauthorised access to user accounts is minimal.

Recommendations
As this is the most secure policy it is recommended that this is applied to users that have access to additional sensitive data or have additional privileges:

- Teachers
- Staff

Password Policy - Fair

Attribute	Strong
Password History Length	5
Password Complexity Status	FALSE
Minimum Password Length	5 Characters
Minimum Password Age	0 days

Maximum Password Age	365 days
Lockout Threshold	5 invalid logon attempts
Lockout Observation Window	30 minutes
Lockout Duration	30 minutes

Composition
This policy would require the user to have at least a 5 digit password made up of any characters. This cannot be the same as the previous 5 passwords.
The password will expire after a year.
The account will lockout after 5 invalid attempts, but will automatically unlock after 30 minutes.

Security
This is fairly simple to use and in terms of security this policy is fair/moderate, as the risk is lower for unauthorised access to user accounts.

Recommendations
As this is not a high security risk policy and not too complex to use it is recommended that this policy is applied to:

- Students (Non SEN)
- Parents
- Visitors

Password Policy - Weak

Attribute	Strong
Password History Length	5
Password Complexity Status	FALSE
Minimum Password Length	5 Characters
Minimum Password Age	0 days
Maximum Password Age	365 days
Lockout Threshold	5 invalid logon attempts
Lockout Observation Window	30 minutes
Lockout Duration	30 minutes

Composition
This policy would require the user to have at least a 4 digit password made up of any characters and can be the same as any previous passwords.
The password does not expire and does not lockout if entered incorrectly.

Security
Although this policy is easy to use, in terms of security this policy is weak, as there is a high risk of unauthorised access to user accounts, due to the simplicity of the structure.

Recommendations
Due to the high security risk it is recommended that this policy is applied to SEN students only. But if required can be applied to any user.

General expectations:

- 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 to Newfield School and Blackburn with Darwen environment by locking the workstation when it is not in use so that casual overlooking and unauthorised tampering is prevented (for guidance on how to lock your screen please contact the IT Department).
- 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 IT Department.
- 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.
- Lock the workstation when it is not in use and 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.

Appendix 3 - ICT Asset Protocol

1. Where any ICT Asset (any school ICT equipment) is taken outside the Site it shall be checked out by the relevant person upon leaving the Site and checked in upon return using a system that shall be agreed by the school.

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 WAN.

4. In consultation with the school, any person who is reasonably suspected of breaching this protocol may be denied permission to remove ICT Assets from the Site.

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

6. The Authority shall use reasonable endeavours to ensure that staff and students are informed of all further rules and procedures established to protect the security of ICT Assets.

7. Where any ICT Asset not on long term loan is taken outside the Site it shall be checked out by the relevant person upon leaving the Site and checked in upon return using a system that shall be agreed by school.

8. 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 Newfield School 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.

Appendix 5 - 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;
Computer Misuse Act 1990;
Copyright, Designs and Patents Act 1988
General Data Protection Regulation (GDPR) (2018)

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

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 Head teacher 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 Newfield School 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.

General Data Protection Regulation (GDPR) (2018)

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Appendix 6 – Acceptable 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 the Newfield School 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 the Newfield School 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 the Newfield School 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 Newfield ICT network without the specific agreement of the Head teacher and/or IT Department.
- 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 office 365 mail servers, or referencing an email address hosted on 365 mail systems.
• Failing to observe intellectual property
• Keeping, accessing or transmitting confidential data about other students.
• Producing documents or 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 Newfield 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 Newfield School ICT systems,
• Using school 365 email or messaging systems to engage in inappropriate or non-professional communications between either staff, staff and students or students
• Any uses of school ICT equipment of personal gain.

Appendix 7 – Other Related Policies

- Safer Recruitment
- Anti-Bullying
- Health and Safety
- Equal Opportunities
- Community Cohesion
- Children Looked After
- Educational Visits
- Missing Children
- Grievance and Disciplinary
- CPD
- E Safety
- Racist Incidents
- Whistle Blowing
- Security
- Curriculum
- Recruitment and Selection
- Managing Allegations
- Data Protection