Avondale Primary School

ICT and Acceptable Use Policy

Policy Written by Blackburn with Darwen and Vicky Brown
Accepted the Governing Body Autumn 2026
To be reviewed Autumn 2028

Contents

1. Introduction
- **1.1** Purpose
- **1.2** Objective
- **1.3** Definitions
- **1.4** Scope
- **1.5** Expectations

2. Compliance
- **2.1** All Users
- **2.2** School Staff
- **2.3** Temporary Users
- **2.4** Operations & Authority Staff

3. ICT Security
- **3.1** Governing Body Responsibilities
- **3.2** Internal Audit Responsibilities
- **3.3** Head Teacher Responsibilities
- **3.4** School Responsibilities
- **3.5** User Accounts
- **3.6** Equipment Sitting
- **3.7** All User Responsibilities
- **3.8** Staff Users additional Responsibilities
- **3.9** BSF ICT Service Provider Responsibilities

4. Online Communication and use of the web
- **4.1** Provision
- **4.2** Guidance on Use

5. Portable Devices and External Connections
- **5.1** External Network Connections
- **5.2** Removable Media, Mobile Devices and Cloud Storage
- **5.3** Devices connected to the BwDB ICT Network

6. Storage and installation of Software, Resources and Data
- **6.1** Licenses
- **6.2** Data Ownership
- **6.3** Protection of Data

7. Dealing with incidents of unacceptable or inappropriate use
- **7.1** Systems and Security Monitoring
- **7.2** Reporting
- **7.3** Consequences
- **7.4** Incident Response Investigations

8. Policy Review

Appendix 1 **Staff Information Systems Code of Conduct**
Appendix 2 **Password Security Guidance**
Appendix 3 **ICT Asset Protocol**
Appendix 4 **Information Classifications**
Appendix 5 **Data Protection and Other Relevant Legislation**
Appendix 6 **Unacceptable Use**

1 Introduction

This policy outlines the secure and safe use of computer equipment on the shared Avondale Primary School and BWD network.

Avondale Primary School and BWD LA and are committed to protecting employees, partners and students from illegal or damaging actions by individuals, either knowingly or unknowingly. Avondale Primary School and Local Authority will take appropriate steps to protect ICT equipment, resources and environments 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 Avondale Primary School ICT resources and equipment.
- Ensure all use of the ICT resources and equipment is legal, ethical, and consistent with the aims, values and objectives of the BWD LA and Avondale Primary School.
- Inform all users of their personal responsibilities when using the school and LA ICT resources and equipment and environment.
- To protect the BWD LA and Avondale Primary School IT environment from all threats whether internal or external.
- To ensure that those who use LA or school ICT resources, equipment and networks are aware of the requirements of IT Security and Acceptable Use.
- To ensure that users are aware of their roles and responsibilities in applying, enforcing and complying with ICT Security and Acceptable Use.

1.2 Objectives

The objectives of this policy are:

- to ensure that equipment, data and staff are adequately protected on a cost-effective basis against any action that could adversely affect the school;
- to ensure that staff users are aware of and fully comply with all relevant legislation and guidance around ICT security and safe and acceptable use of ICT;
- 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 mainframe computer, minicomputer, microcomputer, personal computer (whether hand-held laptop, portable, stand-alone, network or attached to a mainframe computer), workstation, word-processing system, desk top publishing system, office automation system, messaging system, any other similar device and peripherals for these devices.
- ICT environment means any virtual, online, networked or computer based resource or facility available through the school or LA.
- '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's ICT systems and/or data.

1.4 Scope

This policy applies to all users of Avondale Primary School and Blackburn with Darwen LA ICT environment and equipment, 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 devices belonging to staff and pupils. It also covers:

- All equipment that is owned or leased by Avondale Primary School or BWD LA.
- Guest devices authorised by Avondale Primary School or BWD.

- All employees, contractors and temporary staff, outsource agents and other workers at Avondale Primary School or BWD LA who are responsible for the administration and management of the Avondale Primary School ICT equipment and resources.
- All those who use the Avondale Primary School ICT services including both students and staff.

1.5 Expectations

The appropriate Acceptable Usage Agreement should be signed by all staff and pupils, and a parent or guardian of each pupil. A signed AUA form should be returned before a user is permitted access to ICT equipment and services. Signed AUPs are stored safely in the School Office**.** All school staff have a responsibility to familiarise themselves with the relevant sections of this policy before using the Avondale Primary School or BWD LA ICT equipment and environment. Each staff user must read, understand and sign to verify they have read and accepted this policy before using the ICT equipment and environment. **See appendix 1.**

Any user found to have breached the terms of this policy, may be subject to the Avondale Primary 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 ICT environment is provided to support learning within BWDB education system. All those accessing the Avondale Primary School ICT environment 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. If in any doubt, the user should seek advice from the Head Teacher.

2.1 Compliance with Policy for all users

The Avondale Primary School 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 a safeguarding issues arise. In the first instance, for SIMs this would be the School Business Manager and the ICT Technician for other breaches. They would then ensure that this is reported to the Headteacher. Where use may be illegal or result in misconduct proceedings, please refer to the illegal misuse of ICT Flowchart (Appendix 8)

The ICT resources and equipment are provided primarily for the purpose of conducting and supporting learning and teaching activities; however personal usage of school, LA or personal equipment is permitted as long as that does not:

- Take place during lesson time or otherwise interfere with the user's professional role.
- Bring the Local Authority or Avondale Primary School into disrepute.

All users should be aware that usage may be monitored and/or recorded; misuse of the ICT equipment and environment may lead to disciplinary action. In such situations, the Head Teacher and Local Authority will be the arbiters of whether or not the use was reasonable in the circumstances.

2.2 Compliance with Policy for all 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 pupils' accounts, in order to assist the pupil in using the ICT resources and equipment.
- It is acceptable for a member of the school staff to access a student's files.
- Members of the school staff should not use any other users ICT Service user account login for work or personal matters.
- Whilst legally school staff have a right to delete files considered to be inappropriate that are on a pupil's personal device, members of staff do not delete content of files from devices. Correct procedure is to report this to the E-Safety Lead
- http://www.education.gov.uk/aboutdfe/advice/f0076897/screening,-searching-and-confiscation/screening-searching-and-confiscation

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

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

3 ICT Security

A number of different groups have responsibility within Avondale Primary School ICT for aspects of ICT 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 Headteacher.

3.2 Headteacher 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's 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's ICT facilities are applied and documented as an integral part of the Policy.

The Headteacher, in accordance with the School's 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 a named member of school or technical staff, who will keep an inventory of equipment within their remit.

The Headteacher is also responsible for ensuring that the requirements of the UK General Data Protection Regulation (GDPR) and the Data protection Act 2018 (DPA) (Appendix 5) are complied with fully by the school. This is represented by an on-going responsibility for ensuring that the:

- Registrations under the GDPR and DPA 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.

In addition, the Headteacher 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.

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's approved ICT Security Policy/AUP are complied with, and for investigating any suspected or actual breaches of ICT security.

Specialist advice and information on ICT security may be obtained from Head of Audit and Assurance Audit and Assurance 01254 585630 and The Information Governance and IT Compliance Manager 01254 585226.

3.4 School Responsibilities

The Governing Body and Headteacher 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's 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 LP and IMS.
- 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 account for staff, who will be required to comply with minimum password standards and pupils have a common password but are taught the importance of securing their documents. **See appendix 2 for guidance on standards for passwords.**

- Enabled user accounts are available only for current staff and pupils.
- The user account of anyone who is under investigation for inappropriate use of the system must be disabled promptly.
- '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 user's data may be given in exceptional circumstances. Should this be required users should seek advice from the Head Teacher.

3.6 Equipment siting

Reasonable care must be taken in the siting of computer screens, keyboards, printers or other similar devices. Whenever 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 know the information. Specific consideration should be given to the siting of devices on which confidential, **special category 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 **special category or sensitive** data are not left unattended on desks;

The same rules apply to school equipment in use at a user's home or when accessing **special category or sensitive** data using home equipment.

3.7 All users responsibilities

All users will sign a user agreement at an appropriate level, before using the school's ICT equipment.

All users of the school's 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**. Pupils will sign an appropriate acceptable use agreement and should be guided by school staff towards respecting and conforming to the expectations of this policy.

All users are responsible for:

- The use of their unique logon details (usernames and passwords), email address where provided 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 a user's account remains protected at all times. See guidance document in Appendix 2.
- Reporting concerns over password security immediately.
- Users are responsible for notifying the Head Teacher 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.
- Ensuring pupils in their care are reminded regularly of expectations around appropriate use of ICT equipment security and E-Safety.
- Returning portable equipment signed out to them for updates when requested to do so.
- Endeavouring to protect Avondale Primary School equipment and the network against Viruses, Malware and other forms of software based attacks by virus checking portable devices and following only reliable, known links.
- Reporting any inappropriate use of ICT services (see section 7).
- Following the ICT Asset Protocol when taking any school or BWD LA ICT equipment off the schools premises.
- Users should report any incidents, either perceived or real, to the Head Teacher at their school. The Head Teacher is responsible for escalating such incidents to LA, technical support service, Internal Audit or other organisation as appropriate.
- All staff should ensure all personal data (pupil/parent/staff) held and used by them is either returned to school ownership or destroyed when leaving employment. Failure to do this may constitute a breach of data protection rules by Avondale Primary School

Users should not make any attempt to disable or reconfigure any ICT security measures or software, including Anti-virus software or seek to bypass any monitoring, filtering or security measures that are in place. **Attempting to do so is expressly forbidden.**

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

3.8 Staff users additional responsibilities

Where users have access to **special category or sensitive** data, they will receive training on data security before accessing data at an appropriate level on the managed service network.

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 ICT equipment security and E-Safety.
- Returning portable equipment signed out to them for updates when requested to do so.

3.9 School technical support

At Avondale Primary School we insist that all technical support staff fully understands and complies with the requirements of GDPR, the DPA and all legislation around the control and storage of data. Crystal has/have responsibility for:

- Ensuring all data held on the curriculum server is backed up and this process meets Government baseline security criteria.
- Bringing any security incidents, either perceived or actual, to the attention of the Head Teacher.
- Management of the ICT network, ICT equipment, systems and data including controlling access to these assets under the instruction of The Head Teacher.
- Integrity of data during both repairs 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.
- 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.

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

4.1 Provision

Internet access

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 LA. Where a user's job role requires them to access sites that may be considered inappropriate approval must be obtained from their Head Teacher prior to access.

Staff with access to the BWD Schools or LA email should be aware that the content of emails and attachments may need to be disclosed under the GDPR and DPA (see Appendix 5) and the Freedom of Information Act 2000. Email use is filtered and can be recorded.

The BWD Learning Platform provides facilities for publication on the World-Wide Web for school-related information, tools to communicate across the school community and tools to upload and publish ideas and resources.

Communication through the Learning Platform may be permitted, but pupils will receive E-Safety education before using the system (for further information, please see E-Safety Policy).

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 a 'blackburn.gov' or 'blackburn.sch' email address when sending, receiving or forwarding emails containing RESTRICTED information.
- Access news groups, bulletin 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 by 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, **special category or sensitive** information (therefore classified as PROTECT or RESTRICTED information - see Information Classifications Section) from blackburn.gov/blackburn.sch email addresses 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/blackburn.sch email accounts. *This should be done through your standard school email address with appropriate encryption. Contact the BT&IT*
- Using the LA and AVONDALE PRIMARYSchool 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 their responsibility to consult the Head Teacher).

5 Portable Devices and External Connections

Facilities are in place to allow the transfer of information into and out of the Avondale Primary 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. Outside visitors are not permitted to use pen drives into computers.

5.1 External Network Connections

Requests for external connections to access the LA ICT Network, must be brought to the attention of BWD LA representatives and BT/IT, who will establish whether it is safe to permit such access.

5.2 Removable Media, Mobile Devices and Cloud Storage

Securing PROTECTED or RESTRICTED data is of paramount importance – particularly in relation to the LA and Avondale Primary School need to protect data in line with the requirements of GDPR and the Data Protection Act 2018. When using portable devices and removable media:

- Permission should be sought from the Head Teacher and an assessment of risks, especially relating to information assurance, should be carried out before taking mobile devices out of the school site or using cloud technology to store work related information.(Appendix3)
- Users should sign to acknowledge receipt of loan devices.

Wherever possible the preferred method for offline storage/transfer should be via One Drive, available as part of School's Office 365 applications.

Users should not engage in the following activities when using cloud storage, 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 LA 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.
- **All devices MUST be encrypted – this is a minimum standard expected by the Information Commissioner's Office (ICO) for devices used to hold personal data**

5.3 Devices connected to the BWD or school ICT network

Any device connected to the BWDLA or Avondale Primary School ICT 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 Head Teacher before guest devices can be connected to the school network.

Any loss or theft of removable media or portable devices must be reported immediately to the Head Teacher. **If the device contains personal data the School's Data Protection Officer should also be notified and a data breach form completed**.

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 must be followed. **See Appendix 5**

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 Avondale Primary 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 school's responsibility to ensure that all software on the ICT 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.
- The LA and 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 is strictly prohibited.
- It is the school's responsibility to ensure that software added to all devices and desktops 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 Avondale Primary School ICT environment will be owned by a number of different individuals and organisations. BWD LA 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 GDPR and the DPA, 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 Local Authority and 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.

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:

- The blackburn.gov email system is filtered and recorded
- Web usage is actively filtered and recorded
- System usage may be recorded
- System files, etc. may be accessed to ensure confidentiality integrity and availability.
- All users are responsible for the security of 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 mobile ICT equipment and the BWD Learning Platform and encouraged to support their child in fulfilling the expectations.
- Any 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.

7.2 Reporting

Any inappropriate or unacceptable use of the school ICT equipment, resources or personal devices during school time should be reported to the appropriate organisation.

7.3 Consequences

Avondale Primary School or 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 or LA will decide on the appropriate disciplinary action.

- The Incidence Response Protocol is followed where inappropriate or illegal material may be present on school equipment
- Incidents are recorded in the correct section of the incident log by the Headteacher
- The LA is informed of sites that need to be blocked (E learning Team)
- Internal Audit are informed of any potential security breach
- Appropriate investigations disciplinary procedures are followed.

School and the Local Authority reserve 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 or LA will decide on the appropriate disciplinary action.

Any violations of this security policy should initially be brought to the attention of the Head Teacher. Violation of this security policy by a member of school staff may lead to disciplinary proceedings and/or legal proceedings against that individual. Intentional or persistent violation of this security standard by staff of third parties in a contractual relationship with Avondale Primary School, will be treated as a breach of the appropriate contract. Where a pupil is involved in intentional persistent violation of this policy, appropriate action will be taken by the Head Teacher.

7.4 Incident Response Investigations

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. All security incident reports and logs must remain confidential and only authorised personnel will be permitted to view this material. 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.
The LA/ local law enforcement agency will be contacted if the severity of a security breach necessitates this course of action.

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.
- Rogue software or hardware appearing on the Avondale Primary School network.

8 Policy review

This policy will be reviewed by Avondale Primary 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.

Reviewed and updated Autumn 2026
Next review date: Autumn 2027

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 E-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 GDPR and the Data Protection Act of 2018 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 E-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 not use the Carbon Copy (CC) function on email inappropriately. Use must be proportionate and relevant.
- I will only use my Avondale Email account for school business.
- The sending of emails should be limited to business hours (8:00am to 5:00pm) wherever possible. Any messages sent outside of these hours should not be sent with the expectation of an 'out of hours' reply. You are also not expected to reply to any messages received 'out of hours'.
- I will promote e-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. As a minimum a strong password contains a mixture of numbers, letters and punctuation. Alternatively, you can use a passphrase where you group three random words together, adapting this for the requirements of the specific system being used such as adding a special character, capital letter or number.
- Never reveal your passwords to anyone (includes colleagues, BT&IT Service Desk, Line Managers, family and friends)
- Passwords should be changed on a regular basis.
- 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 where this is possible and report your concern to the Head Teacher.
- 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.

- Where pupils have individual passwords, they should not share these with others and inform their teacher if they believe it has been compromised.
- Where pupils share a common login, they should be taught the importance of treating other pupils work with respect and keeping their group password secure.

Appendix 3 - ICT Asset Protocol

Where any ICT Asset (any school or LA ICT equipment) is taken outside the site it must be checked out by the relevant person upon leaving the Site and checked in upon return.

Whilst any ICT Asset is outside the Site:

- the person who checked it out shall be responsible for taking all reasonable precautions and care of it and for its safe return;
- 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;
- 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.
- it shall not be used where there is any material risk of damage from liquids, impact or otherwise;
- it shall not be lent or entrusted to any other person;
- 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.

In using any ICT Asset:

- users shall not attempt to modify or circumvent any antivirus or other security software;
- 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;
- Users shall comply with the Acceptable Use Policy when accessing the Wide Area Network.

Any person whom the school reasonably suspects may be in breach of this protocol may be denied permission to remove ICT Assets from the Site.

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

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

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.

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 **special category or 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 AVONDALE PRIMARY 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 :-

UK General Data Protection Regulation;
Data Protection Act 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 UK General Data Protection Regulation and the Data Protection Act 2018

The UK General Data Protection Regulation and the Data Protection Act 2018 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 6, *integrity and confidentiality,* 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 GDPR and Access to Information procedures.

5.2.1 To be able to meet the requirements of the GDPR and the DPA, the Head Teacher is required to compile a list of processing, giving details and usage of all relevant personal data held on computer within the school and notify the Information Commissioner of their processing. It is important that amendments are submitted where the scope of the system extends to new areas of operation. The GDPR and DPA 2018 are consistent with the principles established in the 1998 Act.

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.

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 AVONDALE PRIMARYSchool 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 the AVONDALE PRIMARY 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 (including for political, extremist purposes).
- Hacking, probing, scanning or testing the weaknesses of a system within the AVONDALE PRIMARY 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 AVONDALE PRIMARY 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 ICT network without specific agreement.
- 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 emails or messages which are excessive and/or intended to harass or annoy others. This includes sending large numbers of messages
- Sending, or attempting to send, spam of any kind from third-party networks using a return email address that is hosted on the ICT mail servers, or referencing an email address hosted on the BSF ICT 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 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 AVONDALE PRIMARY School ICT systems,
- Using managed service 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 equipment connected to the network, intended to bully or harass others.