WALTON HIGH SCHOOL

Proud to be part of Walton Multi Academy Trust

EXAMINATION CONTINGENCY POLICY

Date Established: January 2026
Review Date: January 20207
Leadership Link: Deputy Headteacher Exams

Walton Multi Academy Trust refers to all schools within the Trust.
When referring to Trust Boards, this includes Local Governor Boards, and the term 'Governor' includes all Trustees or Local Board Governors.

Contents

Purpose of the Plan

Risk Factor 1. Examinations Officer extended absence at key points in the Examinations Cycle.
Risk Factor 2. SENCO extended absence at key points in the exam cycle.
Risk Factor 3. Teaching staff extended absence at key points in the exam cycle.
Risk Factor 4. Invigilators - lack of appropriately trained invigilators or invigilator absence.
Risk Factor 5. Disruption to Public Transport preventing students from reaching Exams Centre.
Risk Factor 6. Candidates unable to take examinations because of a crisis – centre remains open
Risk Factor 7. Centre unable to open as normal during the exams period.
Risk Factor 8: Failure of IT systems/AI Misuse.
Risk Factor 9: Lack of appropriate rooms or main venues unavailable at short notice
Risk Factor 10. Disruption to the distribution of examination papers.
Risk Factor 11: Disruption to the transportation of completed examination scripts
Risk Factor 12: Assessment evidence is not available to be marked
Risk Factor 13: Centre unable to distribute results as normal
Risk Factor 14: Cyber Security

Examinations Contingency Plan

Purpose of the Plan

This plan examines potential risks and issues that could cause disruption to the management and administration of the exam process at Walton High School. By outlining actions/procedures to be followed in case of disruption it is intended to mitigate the impact these disruptions have on our exam process. This has been written in accordance with JCQ Guidance: Disruption_Planning_24_FINAL.pdf

Risk Factor 1: Examinations Officer extended absence at key points in the examination cycle
The following are the key tasks involved in the management and administration of the examination cycle which would be at risk in the event of the Examinations Officer being absent:

Planning
• annual data collection exercise not undertaken to collate information on qualifications and awarding body specifications being delivered.

• annual exams plan not produced identifying essential key tasks, key dates and deadlines.
• sufficient invigilators not recruited and trained.

Entries
• awarding bodies not being informed of early/estimated entries which prompts release of early information required by teaching staff
• candidates not being entered with awarding bodies for external exams/assessment
• awarding body entry deadlines missed or late or other penalty fees being incurred

Pre-exams
• exam timetabling, rooming allocation; and invigilation schedules not prepared
• candidates not briefed on exam timetables and awarding body information for candidates
• exam/assessment materials and candidates' work not stored under required secure conditions
• internal assessment marks and samples of candidates' work not submitted to awarding bodies/external moderators

Exam time
• exams/assessments not taken under the conditions prescribed by awarding bodies
• required reports/requests not submitted to awarding bodies during exam/assessment periods e.g. very late arrival, suspected malpractice, special consideration
• candidates' scripts not dispatched as required to awarding bodies.

Results and post-results
• access to examination results affecting the distribution of results to candidates
• the facilitation of the post-results services

Contingency for key staff absence:

• The Examinations Officer will take over the role of the Exams Manager in the event of the Examination Manager absent, and vice versa:
Claire Collins will cover Maggi Beddoes if absent
Maggi Beddoes will cover Claire Collins if absent
In the event that both the Exams Officer and Exams Manager are absent at the same time, the contingency is as follows:

Exam Papers/Venues – Susan Kumar-Merino
Download of exam papers/audio files – Damian Walton

• The SLT should nominate a "Deputy" to cover a role or task/Senior Invigilator: R Kileen to cover S Barker if absent.
• • All procedures are documented and are available on sharepoint

Key documents can be found at:

The Key Tasks section of The Exams Office website.
- The Examinations Oracle and Centre Support Service of the Examination Officers Association.
- The Examinations Administration section of the DFE website.
- Examination Board helplines.
- The Exams Office section of the Joint Council for Qualifications website.

Examinations Contingency Plan

Risk Factor 2: SENCO extended absence at key points in the exam cycle

Key tasks required in the management and administration of the access arrangements process within the exam cycle not undertaken including:

Planning
- candidates not tested/assessed to identify potential access arrangement requirements
- evidence of need and evidence to support normal way of working not collated

Pre-exams
- approval for access arrangements not applied for to the awarding body
- modified paper requirements not identified in a timely manner to enable ordering to meet external deadline.
- staff providing support to access arrangement candidates not allocated and trained.

Exam time
- access arrangement candidate support not arranged for exam rooms.

Contingency Procedure:
- Request SENCO Assistant to take over until SENCO returns – A Cashmore LG SEND Link / C Musker HLTA to cover in the event of SENDCO J Byrne absence.
- SENCO support staff to identify any candidates not yet approved by Awarding Bodies and complete.
- Examinations Officer/Manager to identify any shortfalls in Invigilation requirements and ensure that gaps are filled.
- Once gaps are filled, Examinations Officer/Manager to arrange suitable rooms and SENCO to provide training.
    - Access Arrangements Coordinator C Boston to cover in the event of SENDCO absence andf work with the Exams Manager to implement access arrangements, and vice versa J Byrne to cover in the event of C Boston's absence.

Risk Factor 3: Teaching staff extended absence at key points in the exam cycle

Key tasks not undertaken including:
- Early/estimated entry information not provided to the exams officer on time; resulting in pre-release
- information not being received
- Final entry information not provided to the exams officer on time; resulting in:
- candidates not being entered for exams/assessments or being entered late
- late or other penalty fees being charged by awarding bodies

- Internal assessment marks and candidates' work not provided to meet submission deadlines

Contingency Procedure:
• Head of Department and / or Second in Department or SLT Link member to provide Examinations Officer/Manager with details of Estimated/Final entries by exam board deadlines.
• Subject Head of Department or SLT member to ensure Examinations Officer/Manager is provided with Estimated Grades/Coursework Marks and that Coursework samples are transmitted to Moderators.

Examinations Contingency Plan

Risk Factor 4: Lack of appropriately trained invigilators or invigilator absence

- Failure to recruit and train sufficient invigilators to conduct exams
- Invigilator shortage on peak exam days
- Invigilator absence on the day of an exam

Contingency Procedure:

- Examinations Officer/Manager to maintain a team of suitable Invigilators which can be called upon in the event of a shortfall (if available).
- Conduct a review of available invigilators and their availability for the next exams series.
- Use provisional timetable and estimated entry information to determine invigilator numbers required.
- Identify where invigilators may be short and recruit to meet legal requirements.
- Request permission to recruit additional invigilators
- SLT member responsible for Cover to provide additional Invigilator resource in the event of a shortfall at short notice.
- Staff agencies to be contacted if none of the above is successful.

Risk Factor 5. Disruption to Public Transport preventing students from reaching Exam Centre.

- Candidates unable to take examinations due to planned lack of public transport.
- Candidates unable to take examinations due to sudden disruption to public transport.
- Candidates arrive late due to public transport problems.

Contingency Procedure:

- Monitor news agencies on a regular basis to identify any potential transportation difficulties.
- Centre to utilise own bus facilities to transport candidates to centre if possible.
- Centre to liaise with candidates to identify whether the examination can be sat at an alternative venue in agreement with the relevant awarding organisations.
- Centres to offer candidates an opportunity to sit any examinations missed at the next available series.
- Centres to apply to awarding organisations for special consideration for candidates where they have met the minimum requirements.
- Latecomers to be permitted to take their examinations providing they are within the JCQ regulations.

Risk Factor 6: Candidates unable to take examinations because of a crisis – centre remains open

- Candidates are unable to attend the examination centre to take examinations as normal

Contingency Procedure:

- Centre to liaise with candidates to identify whether the examination can be sat at an alternative venue in agreement with the relevant awarding organisations (Alternative venues to be used: Berkswich Methodist Church & Local Schools within our MAT Academy.
- Centres to offer candidates an opportunity to sit any examinations missed at the next available series.
- Centres to apply to awarding organisations for special consideration for candidates where they have met the minimum requirements. Candidates are only eligible for special consideration if they have a medical certificate or have been advised by their centre not to attend an examination.
- If a candidate chooses not to sit an examination they should be aware that special consideration rules will not apply.
- JCQ guidance on special consideration can be accessed through the JCQ website.

Examinations Contingency Plan

Risk Factor 7: Centre unable to open as normal during the exams period

- Centre closed or candidates are unable to attend for an extended period.
- The provision of normal teaching and learning is interrupted.
- Centre closed due to inaccessibility or risk of injury caused by severe weather.

Contingency Procedure:

- It remains the responsibility of centres to prepare students, as usual, for examinations.
- In the event that the head of centre decides the centre cannot be opened for scheduled examinations the relevant awarding body must be informed as soon as possible.
- Awarding bodies will be able to offer advice regarding the alternative arrangements for conducting examinations that may be available and the options for candidates who have not been able to take scheduled examinations.
- The centres to open for examinations and examination candidates only, if possible
- Local MAT Primary Schools will be used in the event that candidates cannot sit exams at the Centre.
- Centres may advise candidates to sit examinations in an alternative series.
- Special Consideration can be used where candidates are unable to achieve a result due to one of the above factors.
- An exam result can be generated by the awarding body, based on factors such as a child's performance on other assessments in the same subject.

Risk Factor 8: Failure of IT systems

- MIS system failure at final entry deadline
- MIS system failure during exams preparation
- MIS system failure at results release time

Contingency Procedure:

- Awarding bodies to be informed of the situation and an extension to the deadline should be requested.
- MIS contractor and ICT team on standby to repair damage quickly.
- Special Consideration can be applied for in the event of a serious disruption.
- Results can be obtained at an alternative site.

Misuse of AI (Artificial Intelligence)

AI plagiarism by any student or staff member will be escalated in Centre for investigation by a senior member of leadership team responsible to examinations. They will consult with the IT Manager as to whether they deem AI plagiarism malpractice has occurred and then this will be reported back to the Exams Manager/Officer for the appropriate action with the relevant examination board(s) and appropriate sanctions will be imposed.

Examinations Contingency Plan

Risk Factor 9: Lack of appropriate rooms or main venues unavailable at short notice

- Exams officer unable to identify sufficient/appropriate rooms during exams timetable planning.
- Insufficient rooms available on peak exam days
- Main exam venues unavailable due to an expected incident at exam time

Contingency Procedure:
- Identify, working with responsible SLT member, a short – list of suitable rooms including reserves.
- Move pupils from normal classrooms for the duration of the examinations.
- Plan alternative accommodation for the duration of the incident.

Risk Factor 10. Disruption to the distribution of examination papers.

- Disruption to the distribution of examination papers to centres in advance of examinations.

Contingency Procedure:
- Awarding organisations to provide centres with electronic access to examination papers via a secure external network.
- Awarding organisations may be able to fax examination papers to centres if electronic transfer is not possible.
- The Examinations Officer would need to ensure that copies are received, made and stored under secure conditions
- Source alternative couriers for delivery of hardcopies.

Risk Factor 11: Disruption to the transportation of completed examination scripts

- Delay in normal collection arrangements for completed examination scripts

Contingency Procedure:
- In the first instance centres to seek advice from awarding organisations and normal collection agency regarding collection. Centres are not to make their own arrangements for transportation without approval from awarding organisations.
- Centres to ensure secure storage of completed examination papers until collection.

Risk Factor 12: Assessment evidence is not available to be marked

- Large scale damage to or destruction of completed examination scripts/assessment evidence before it can be marked

Contingency Procedure:
- Awarding organisations to generate candidate marks for affected assessments based on other appropriate evidence of candidate achievement as defined by the awarding organisations
- Candidates to retake affected assessment at subsequent assessment window.

Examinations Contingency Plan

Risk Factor 13: Centre unable to distribute results as normal

• Centre is unable to access or manage the distribution of results to candidates, or to facilitate post results services.

Contingency Procedure:
• Centre to make arrangements to access its results at an alternative site.
• Centre to make arrangements to coordinate access to post results services from an alternative site.
• Centre to share facilities with other centres if this is possible.
Alternative sites that could be utilised include Berkswich Methodist Church and local schools within our MAT Academv.

Further guidance to inform and implement contingency planning:

OFQUAL

Joint Contingency Plan in the event of widespread disruption to the Examination System in England, Wales and Northern Ireland http://dera.ioe.ac.uk/16235/1/2012-12-11-joint-contingency-plan-november-2012.pdf

GOV.UK

Emergencies and severe weather: schools and early years settings https://www.gov.uk/emergencies-and-severeweather-schools-and-early-years-settings
Teaching time lost due to severe weather conditions https://www.gov.uk/government/publications/teaching-timelost-due-to-severe-weather-conditions/teaching-time-lost-due-to-severe-weather-conditions
Dispatch of exam scripts guide - Contingency planning https://www.gov.uk/government/publications/dispatch-ofexam-scripts-yellow-label-service/dispatch-of-exam-scripts-guide

JCQ

Guidance on *alternative site arrangements* http://www.jcq.org.uk/exams-office/forms
Instructions for conducting examinations http://www.jcq.org.uk/exams-office/ice---instructions-for-conducting examinations
Guidance on *access arrangements and special consideration* http://www.jcq.org.uk/exams-office/accessarrangements-and-special-consideration

USEFUL INFORMATION

AQA http://www.aqa.org.uk/ JCQ http://www.jcq.org.uk/homepage.cfm
CCEA http://www.rewardinglearning.org.uk/ Ofqual http://www.ofqual.gov.uk/
City & Guilds http://www.cityandguilds.com/ukhome.html
DfE http://www.education.gov.uk/
Edexcel http://www.edexcel.com/Pages/home.aspx
DfE – Exams
Delivery Support
http://www.education.gov.uk/schools/teachingandlearning/qualifications/examsadmin
EDI http://www.ediplc.com/ DENI http://www.deni.gov.uk/
ICAAE http://www.icaa.com/ UCAS http://www.ucas.ac.uk/
OCR http://www.ocr.org.uk/ Welsh Government http://wales.gov.uk/topics/educationandskills/?lang=en
VTCT http://www.vtct.org.uk/
WJEC http://www.wjec.co.uk/
JCQ access arrangements, reasonable adjustments and special consideration.
http://www.jcq.org.uk/exams_office/access_arrangements/
JCQ instructions for conducting examinations
http://www.jcq.org.uk/exams_office/instructions_for_conducting_examinations/
DfE guidance on dealing with disruption to teaching and learning
http://www.education.gov.uk/schools/adminandfinance/emergencyplanning/a0069425/advice-on-severe-weather

Examinations Contingency Plan

Risk Factor 14: Cyber Security

Information and Communications Technology (ICT) Cyber Security Policy

1. Introduction

1.1 We are managing a significant investment in the use of ICT. In many areas of work the use of ICT is vital and must be protected from any form of disruption or loss of service. It is therefore essential that the availability, integrity and confidentiality of the ICT systems and data are maintained at a level that is appropriate for our needs.

1.2 Sufficient resources should be allocated each year to ensure the security of the school's ICT systems and to enable users to comply fully with the legal requirements and policies covered in this Policy. If insufficient resources are available to fully implement this policy, then the potential risks must be documented and reported to Governors by the ICT committee.

2. Policy Objectives

2.1 Against this background there are four main objectives of the ICT Security Policy:-

a) to ensure that equipment, data and staff 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;

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 and students understand the need for ICT security and their own responsibilities in this respect.

d) to safeguard and promote the welfare of students at Walton High School

3. Application

3.1 The ICT Security Policy is intended for all school staff who have control over or who use or support the school's administration and curriculum ICT systems or data. Pupils using the school's ICT systems or data are covered by the relevant 'Rules for ICT Users' and 'E-mail and Internet Use Good Practice' documents, which are incorporated within this policy.

3.2 For the purposes of this document the terms `ICT' (or `ICT system'), `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 (eg mobile phone or MP3 player) or any other similar device;

- `ICT data' means any information stored and processed by ICT and includes programs, text, pictures and sound;

- 'ICT user' applies to any Walton Multi Academy Trust employee, pupil or other authorised person who uses the school's ICT systems and/or data.

4. Scheme of Delegation under the ICT Security Policy

4.1 The ICT Security Policy relies on management and user actions to ensure that its aims are achieved. Consequently, owner, corporate and individual levels of responsibility for ICT security are clearly defined below.

4.2 Owner

4.2.1 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 Walton Multi Academy Trust, which will normally hold it for the benefit of the school.
Exceptions to this will be allowed for software and documentation produced by individual Teachers for lesson purposes – this includes schemes of work, lesson plans, worksheets or as otherwise agreed in writing by the Headteacher.

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

4.3 Governing Body

4.3.1 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. There is a named E-safety governor.

In practice, the day-to-day responsibility for implementing these legislative requirements rests with the Headteacher through the ICT Committee

4.4 Headteacher

4.4.1 The Headteacher is responsible for ensuring that the legislative requirements relating to the use of ICT systems are met and that the school's ICT Security Policy, as may be amended from time to time, 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.

In practice, the day to day functions should be delegated to the ICT Committee, who must be nominated in writing by the Headteacher.

4.4.2 The Headteacher 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 and

- registrations are observed with the school.

4.4.3 In addition, the Headteacher is responsible for ensuring that users of systems and data are familiar with the relevant aspects of the Policy and to ensure that the appropriate controls are in place for staff to comply with the Policy. This is particularly important with the increased use of computers and laptops at home. Staff should exercise extreme care in the use of personal data at home to ensure legislation is not contravened, in particular the Data Protection Act 1998.

4.5 ICT Committee

4.5.1 The ICT Committee is responsible for the school's ICT equipment, systems and data and will have direct control over these assets and their use, including responsibility for controlling access to these assets and for defining and documenting the requisite level of protection. The ICT Committee will consist of employees of the school or the County Council.

4.5.2 Consequently, the ICT Committee will administer 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.

4.5.3 In line with these responsibilities, the ICT Committee will be the official point of contact for ICT security issues and as such is responsible for notifying the Headteacher or Chair of Governors of any suspected or actual breach of ICT security occurring within the school. The Headteacher or Chair of Governors should ensure that details of the suspected or actual breach are recorded and made available to Internal Audit upon request. The Headteacher or Chair of Governors must advise Internal Audit of any suspected or actual breach of ICT security pertaining to financial irregularity.

4.6 Internal Audit

4.6.1 Walton Multi Academy Trust Audit Committee is responsible for checking periodically that the measures prescribed in each school's approved ICT Security Policy are complied with, and for investigating any suspected or actual breaches of ICT security.

4.6.2 Specialist advice and information on ICT security may be obtained from Entrust who will liaise with Internal Audit on such matters.

4.7 Users

4.7.1 All users of the school's ICT systems and data must comply with the requirements of this ICT Security Policy, the relevant rules of which are summarised in `*The Rules for ICT Users'* attached in Annexes C1 – C3.

4.7.2 Users are responsible for notifying the Senior ICT Technician of any suspected or actual breach of ICT security. In exceptional circumstances, users may report any such breach directly to the Headteacher, Chair of Governors or to Internal Audit.

5. 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
The Telecommunications Act 1984

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

5.2.1 The Data Protection Act exists to regulate the use of computerised information about living individuals. To be able to meet the requirements of the Act, the Headteacher is required to compile a census of data giving details and usage of all relevant personal data held on computer within the school and file a registration with the Data Protection Registrar. It is important that amendments are submitted where the scope of the system extends to new areas of operation. The 1998 Act is consistent with the principles established in the 1984 Act, but extends the regulation to certain manual records as well as computerised information.

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 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.

5.4.3 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.

5.4.4 The Senior ICT Technician 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. Users must get prior permission **in writing** from the Senior ICT Technician before copying any software.

5.4.5 The Senior ICT Technician 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.

5.4.6 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.

5.5 The Telecommunications Act 1984 and 2000

5.5.1 The Telecommunications Act 1984, section 43 makes it an offence to send 'by means of a public telecommunications system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character'.

5.5.2 The Telecommunications Regulations 2000 impose restrictions on the interception of communications such as e-mail.

6. Management of the Policy

6.1 The Headteacher should allocate sufficient resources each year to ensure the security of the school's ICT systems and to enable users to comply fully with the legal requirements and policies covered in this Policy. If insufficient resources are available to fully implement this policy, then the potential risks must be documented and reported to Governors.

6.2 Suitable training for all ICT users and documentation to promote the proper use of ICT systems will be provided. Users will also be given adequate information on the policies, procedures and facilities to help safeguard these systems and related data. A record of the training provided through the school to each individual user will be maintained.

6.3 In addition, users will be made aware of the value and importance of such ICT systems and data, particularly data of a confidential or sensitive nature, and be made aware of their personal responsibilities for ICT security.

6.4 To help achieve these aims, the relevant parts of the ICT Security Policy and any other information on the use of particular facilities and techniques to protect the systems or data will be disseminated to users.

6.5 The Headteacher must ensure that adequate procedures are established in respect of the ICT security implications of personnel changes. Suitable measures should be applied that provide for continuity of ICT security when staff vacate or occupy a post. These measures as a minimum must include:-

- a record that new staff have been issued with, have read the appropriate documentation relating to ICT security, and have signed the list of rules;
- a record of the access rights to systems granted to an individual user and their limitations on the use of the data in relation to the data protection registrations in place;
- a record that those rights have been amended or withdrawn due to a change to responsibilities or termination of employment;

7. Physical Security

7.1 Location Access

7.1.1 Adequate consideration should be given to the physical security of rooms containing ICT equipment (including associated cabling). As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data. The server rooms should be locked when left unattended. Ideally,such rooms should have a minimum of key pad access.

7.1.2 The Senior ICT Technician must ensure 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.

7.1.3 Staff have a personal responsibility to ensure the physical security of any hardware provided by the school for their use. In particular laptops, memory sticks and other portable items must be securely stored.

7.2 Equipment siting

7.2.1 Reasonable care must be taken in the siting 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 are 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 or sensitive information is processed or retrieved;
- equipment is sited to avoid environmental damage from causes such as dust & heat;
- users have been instructed to 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;
- users have been instructed not to leave hard copies of sensitive data unattended on desks;

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

7.3 Inventory

7.3.1 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.

8. System Security

8.1 Legitimate Use

The school's ICT facilities must not be used in any way that breaks the law or breaches this policy
Such breaches include, but are not limited to:-

- making, distributing or using unlicensed software or data;
- making or sending threatening, offensive, or harassing messages;
- creating, possessing or distributing obscene material;
- unauthorised private use of the school's computer facilities.

8.1.2 Reasonable private use by staff in their non-contact time is authorised, however staff are encouraged not to abuse this facility and any e-mail and internet use is in accordance with the school's user policy.

8.2 Private Hardware & Software

8.2.1 Dangers can occur from the use of unlicensed software and software infected with a computer virus. It is therefore vital that any private software permitted to be used on the school's equipment is acquired from a responsible source and is used strictly in accordance with the terms of the licence. The use of all private hardware for school purposes must be approved by the Senior ICT Technician.

8.2.2 Staff and students are not encouraged to use private digital cameras/camera phones, but to use school cameras instead. Publication, distribution and storage of these images must be in accordance with this policy.

8.3 ICT Security Facilities

8.3.1 The school's ICT systems and data will be protected using appropriate security arrangements outlined in the rest of Section 8. In addition consideration should also be given to including appropriate processing controls such as audit trails, input validation checks, control totals for output, reports on attempted unauthorised access, etc.
For new systems, it is recommended that such facilities be confirmed at the time of installing the system. Information on the range of such facilities can be sought from the Council's ICT Unit

8.4 Authorisation

8.4.1 Only persons authorised in writing by the ICT Committee, are allowed to use the school's ICT systems. The authority given to use a system will be sufficient but not excessive and the authority given must not be exceeded.
Failure to establish the limits of any authorisation may result in the school being unable to use the sanctions of the Computer Misuse Act 1990. Not only will it be difficult to demonstrate that a user has exceeded the authority given, it will also be difficult to show definitively who is authorised to use a computer system.
All ICT systems should display a message to users warning against unauthorised use of the system.

8.4.2 Access eligibility will be reviewed continually, including remote access for support. In particular the relevant access capability will be removed when a person leaves the employment of the school. In addition, access codes, user identification codes and authorisation rules will be reviewed whenever a user changes duties.
Failure to change access eligibility and passwords will leave the ICT systems vulnerable to misuse.

8.4.3 Temporary access will be granted when necessary through the use of "Guest Accounts" eg a visiting moderator who needs to see student work held on the network

8.5 Passwords

8.5.1 The level of password control will be defined by the Senior ICT Technician based on the value and sensitivity of the data involved, including the possible use of "time out" passwords where a terminal/PC is left unused for a defined period.

8.5.2 Passwords for staff users <u>are recommended to</u> be changed at least termly and should not be re-used. They should be a minimum of 8 alphanumeric characters and not obviously guessable.

8.5.3 Passwords should be memorised. If an infrequently used password is written down it should be stored securely.
Passwords or screen saver protection should protect access to all ICT systems, including "boot" passwords on PCs, particularly laptop/notebook PCs as they are highly portable and less physically secure.
It is acknowledged that the use of 'boot' passwords may not be feasible on Curriculum systems.

8.5.4 A password must be changed if it is affected by a suspected or actual breach of security or if there is a possibility that such a breach could occur, such as:-

- when a password holder leaves the school or is transferred to another post;
- when a password may have become known to a person not entitled to know it.

The need to change one or more passwords will be determined by the risk of the security breach.

8.5.5 Users must not reveal their password to anyone, apart from authorised staff. Users who forget their password must request the Senior ICT Technician issue a new password.

8.6 Backups

8.6.1 In order to ensure that our essential services and facilities are restored as quickly as possible following an ICT system failure, back-up copies of stored data will be taken at regular intervals as determined by the Senior ICT Technician, dependent upon the importance and quantity of the data concerned.

Where programs and data are held on the Council's systems or other multi-user system, such security is likely to be covered by existing procedures. In the case of other ICT systems (including PCs) the user will normally need to make security copies of their data.

8.6.2 Security copies should be clearly marked as to what they are and when they were taken and stored away from the system to which they relate in a restricted access fireproof location and/or off site.

8.6.3 Instructions for re-installing data or files from backup should be fully documented and security copies should be regularly tested to ensure that they enable the systems/relevant file to be re-loaded in cases of system failure.

8.7 Virus Protection

8.7.1 school will use appropriate Anti-virus software for all school ICT systems.
Schools are actively encouraged to conform to the recommended anti-virus protection standards. All Users should take precautions to avoid malicious software that may destroy or corrupt data.

8.7.2 The school will ensure that every ICT user is aware that any PC with a suspected or actual computer virus infection must be disconnected from the network and be reported immediately to the Senior ICT Technician who must take appropriate action, including removing the source of infection.
The governing body could be open to a legal action for negligence should a person suffer as a consequence of a computer virus on school equipment.

8.7.3 Teachers must take the necessary steps to ensure anti-virus protection software on their laptop is updated on a weekly basis as a minimum.

8.8 Disposal of Waste

8.8.1 Disposal of waste ICT media such as print-outs, floppy diskettes and magnetic tape will be made with due regard to the sensitivity of the information they contain. For example, paper will be shredded if any confidential information from it could be derived.
The Data Protection Act requires that adequate mechanisms be used when disposing of personal data.

8.9 Disposal of Equipment

Prior to the transfer or disposal of any ICT equipment the Senior ICT Technician must ensure that any personal data or software is obliterated from the machine if the recipient organisation is not authorised to receive the data. Where the recipient organisation is authorised to receive the data, they must be made aware of the existence of any personal data to enable the requirements of the Data Protection Act to be met. Normal write-off rules as stated in Financial Regulations apply. Any ICT equipment must be disposed of in accordance with WEEE regulations.
The Data Protection Act requires that any personal data held on such a machine be destroyed.
It is important to ensure that any copies of the software remaining on a machine being relinquished are legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.

8.10 Repair of Equipment

8.10.1 If a machine, or its permanent storage (usually a disk drive), is required to be repaired by a third party the significance of any data held must be considered. If data is particularly sensitive it must be removed from hard disks and stored on floppy disk or other media for subsequent reinstallation, if possible.The school will ensure that third parties are currently registered under the Data Protection Act as personnel authorised to see data and as such are bound by the same rules as school staff in relation to not divulging the data or making any unauthorised use of *it.*

9 Security Incidents

9.1 All suspected or actual breaches of ICT security shall be reported to ICT Committee or the Headteacher in their absence, who should ensure a speedy and effective response to be made to an ICT security incident, including securing useable evidence of breaches and evidence of any weakness in existing security arrangements. They must also establish the operational or financial requirements to restore the ICT service quickly.

The Audit Commission's Survey of Computer Fraud and Abuse 1990 revealed that over 50% of incidents of ICT misuse are uncovered accidentally. It is, therefore, important that users are given positive encouragement to be vigilant towards any suspicious event relating to ICT use.

It should be recognised that the school and its officers may be open to a legal action for negligence if a person or organisation should suffer as a consequence of a breach of ICT security within the school where insufficient action had been taken to resolve the breach.

10. E-Mail & Internet Use Policy

10.1 Attached as Annex A is the "ICT User Policy". This policy applies to all school staff, students and third parties who use either or both of these facilities. The conditions of use are explained in the policy. All school staff accessing these facilities must be issued with a copy of the 'Rules for ICT Users – Staff' and 'E-mail and Internet Use Good Practice' documents and complete the user declaration attached to the policy. For all students, the school will ensure that the relevant 'E-mail and Internet Use Good Practice – Rules for ICT Users - Students' document is issued and the consent form is completed by pupils and their parents. In addition copies of the 'E-mail and Internet Use Good Practice - Rules for ICT Users – Third Parties' document and consent form will be issued to all visitors. All of these documents are contained in Annexes C1 – C3.

11. School Website

11.1 Published content and the school web site

The contact details on the Web site will be the school address, e-mail and the telephone number. Staff or pupils personal information will not be published.

The E –safety co-ordinator will take overall editorial responsibility and ensure that content is accurate and appropriate

11.2 Publishing pupils' images and work

Photographs and video clips that include pupils will be selected carefully and will not enable individual pupils to be clearly identified

Pupils full names will not be used anywhere on the Web site in association with photographs (including images published on the plasma screen in the foyer).

Parents will be given the opportunity to decide if they want pictures of their son/daughter to appear on the website. A list of parents who do not require their son/daughter to appear on the website is kept and up-dated regularly by the school.

12. E - Safety

The school has a responsibility to educate and provide support for all users in terms of E – Safety. This will include the following

i. We have a nominated E-safety Co-ordinator an E-safety Governor and an E – Safety Group (made up of Governors, Staff, Parents and Students)

ii. We update our E-safety Policy and Internet Security Policy annually

iii. We have robust Acceptable Use Policies that all users sign up to before they are allowed access to our systems and we include them as part of our network login

iv. We currently use ENTRUST to provide all our internet services including filters and monitoring software

v. We keep and incident log of any inappropriate use flagged up by our monitoring systems, including any measures taken.

vi. Cyberbullying is included in the school's anti-bullying policy

vii. Assemblies on e-safety are held annually

viii. There are posters around ICT suites advertising methods of keeping safe on the internet

ix. E-safety is part of the PSHE Programme and the wider curriculum

x. Students are introduced to "e-safety awareness" during assemblies using CEOP materials and this is reinforced in their ICT lessons and PDS Sessions

xi. Students know how to report any concerns they have

xii. All staff are introduced with an ICT handbook that includes information on safe use of the school network and internet

xiii. The school website contains pages dedicated to e-safety including guidance, policies and copies of all AUPs. There is also a direct link to CEOP on the homepage for students to report incidents directly

xiv. Parent/guardians are offered specific information evenings on e – safety

xv. It is the responsibility of the school to provide staff advice/training on how to protect themselves from online abuse as part of Whole School Staff INSET

Annex A

Walton High School

ICT/E-Safety User Policy

1 Introduction

1.1 Schools are using E-mail and the Internet more and more to support their activities. This E-mail and Internet use policy, which will form part of our ICT Security Policy, contains the rules for using the E-mail and Internet facilities. It applies to all school users who use either or both of these facilities.

1.2 As well as saying what you are not allowed to use E-mail and the Internet for, the policy also provides guidance on the good practices that you should use and the practices that you should avoid.

1.3 The school will periodically review the policy in response to guidance issued by the County Council.

1.4 The policies/Procedures associated with this policy are

Safeguarding Policy	Designated Staff	Mrs A Cashmore
Anti Bullying Policy	Designated Staff	Mrs A Cashmore
DPA/FoI/Information Security	Designated Staff	Mrs K Curtis / Dr I Stec

2 Access to E-mail and Internet services

2.1 Your connection to E-mail or the Internet must be authorised (in writing or in electronic form) by your Senior ICT Technician. All school Internet access will be via an approved Internet Service Provider (ISP). Any variations to this must be authorised in writing by the Headteacher.

2.2 You must choose the ISP's filtering option if one is available.

2.3 The school E-mail and Internet facilities are for business use but we will allow staff to use them privately, as long as it is reasonable. If you use these facilities, you must keep to and not break any of the conditions in this policy.

2.4 The school has the right to monitor E-mails and Internet use. The software we use (SECURUS) monitors use by all users on any PC/laptop connected to the network (including use of school laptops at home)

2.5 If you intentionally access a computer system or information without permission, you are breaking the law under the Computer Misuse Act 1990.

3 Code of Conduct Declaration

3.1 If you use or have access to our E-mail or Internet facilities, you need to read this policy carefully and make sure that you understand it. The school will provide appropriate training. You then need to sign the declaration / consent form (see Annex C1 – C3) to confirm that you have read, understood and will keep to the policy. You must also understand that we may take action against you if you wilfully break the conditions of the policy.

3.2 The school will keep the signed declaration in your personal file. Sometimes, we may ask you to confirm that you still understand and accept the rules.

4 Specific Conditions of Use

4.1 General prohibitions

4.1.1 You must not use, or try to use, our E-mail and Internet facilities to create, distribute or display in any form, any activity that is or may be considered to be against the law or against our rules and policies. In this context, you are not allowed to use the E-mail and Internet facilities for reasons that are:

- pornographic or obscene;
- intimidating, discriminatory (for example; racist, sexist or homophobic) or that break our anti-harassment and equal opportunities policies in any other way;
- defamatory;
- encouraging violence or strong feelings;
- hateful;
- fraudulent;
- showing or encouraging violence or criminal acts;
- unethical or may give us a bad name; or
- a deliberate harmful attack on systems we use, own or run.

4.1.2 If you find or suspect anyone of using the computer system illegally or unethically, you must report it to the E – safety co-ordinator or Headteacher.
On no account should anyone investigate illegal activities, that is the role of the police. Any monitoring of unethical misuse may take place with the written approval of the E – safety co-ordinator or Headteacher.

4.1.3 You must not use the school E-mail or Internet facilities for time-wasting activities, such as chain letters, or for sending private E-mails to everyone on the global address list.

4.2 Computer viruses

4.2.1 It is a crime to deliberately introduce a computer virus, under the Computer Misuse Act 1990. You must not use the school E-mail and Internet facilities for:

- intentionally accessing or transmitting computer viruses or other damaging software; or
- intentionally accessing or transmitting information about, or software designed for, creating computer viruses.

4.2.2 You must scan any material you receive or download from the Internet to make sure it is virus free. The school will ensure that virus protection exists on any standalone or locally networked computers that can access the Internet and train you in its use. You must not E-mail material that has not been scanned to other users. If you find a virus, or you think the material has one, you must immediately break the connection, stop using the computer and tell your Senior ICT Technician.

4.2.3 You must always follow the instructions that your Senior ICT Technician gives you about virus attacks.

4.2.4 If you are not sure how to use the virus protection system, you must get advice from your Senior ICT Technician.

4.3 **Passwords**

4.3.1 You must not tell anyone your password, apart from authorised staff.

4.4 **Other security**

4.4.1 You must not use or try to use the school facilities for:

- accessing or transmitting information about, or software designed for, breaking through security controls on any system;
- breaking through security controls on any system; (including the use of proxy sites) or
- accessing, without permission, any E-mail that is not for you, even if it is not protected by security controls.

4.5 **Publishing information**

4.5.1 You must get authorisation from the Headteacher for any school information that is to be published on the Internet. All schools have web space available for authoring of their own school web site. Images of individuals must have their permission or that of their parent/guardian before publication of the web site (see Annex C2). We will not allow the publishing or editing of Web sites which involve advertising, financial reward or are part of a business.

4.6 **Copyright**

4.6.1 It is illegal to break copyright protection. You could break copyright if you download or transmit protected material through E-mail or over the Internet.

4.6.2 You must not:

- transmit copyright software from your computer to the Internet or allow any other person to access it on their computer through the Internet; or
- knowingly download or transmit any protected information that was written by another person or organisation without getting permission from the owner.
  Permission can be sought via e-mail.

4.7 **Confidential or sensitive information**

4.7.1 You must not break the conditions of the Data Protection Act 1998 when you use the E-mail services of the Internet for transmitting information.
If you need any more advice about these conditions, you should refer to the Policy summary or obtain further information/advice from the Senior ICT Technician.

4.7.2 The Internet E-mail facility is not a secure way of transmitting confidential, sensitive or legally privileged information unless there are special security measures (such as encryption). Without these security measures, Internet E-mail is as insecure as a postcard that you send through the normal post. So, you should make sure that the Internet is suitable for transmitting information that you feel is confidential, sensitive or legally privileged. If you allow anyone to see this type of information without permission, you may be breaking the law.

4.7.3 If you have to transmit any E-mail over the Internet that you think contains confidential, sensitive or legally privileged information, no matter what special security measures you take, you are strongly advised to include the following disclaimer in the E-mail.
'This E-mail (including any attachments) is only for the person it is addressed to. If you are not this person, you must delete this E-mail immediately. If you allow anyone to see, copy or distribute the E-mail, or if you do, or don't do something because you have read the E-mail, you may be breaking the law'. This disclaimer can be set using the 'autosignature' facility where this is available.

4.8 **Bulletin board**

4.8.1 There are 'bulletin boards' (electronic notice boards) on the County Council's Intranet and the SLN Internet site for discussion, social and personal use. These 'bulletin boards' are moderated to ensure appropriate use. The conditions of use in this policy also apply to the bulletin boards.

4.8.2 Neither the school, the LEA nor the County Council is responsible for the content of any material included in the bulletin board or for anything users do because of the material.

5 **Recording Internet use**

5.1 You should be aware that use of ISP facilities is logged.

5.2 If you access a prohibited Internet site unintentionally, you must break the connection immediately and report it to your Senior ICT Technician or Headteacher. If you do not do this, the school may take action against you.

5.3 You should protect yourself by not allowing unauthorised people to use your Internet facility.

6 **E-mail good practice**

6.1 Annex C1 – C3 contains guidelines that tell you what is and what is not good practice when you use internal or Internet E-mail services.

Misuse of AI (Artificial Intelligence)

AI Plagiarism by any student or staff member will be escalated in Centre for investigation by a senior member of leadership team responsible to examinations. They will consult with the IT Manager as to whether they deem AI Plagiarism malpractice has occurred and then this will be reported back to the Exams Manager/Officer for the appropriate action with the relevant examination board(s) and appropriate sanctions will be imposed.