Information Security Policy

Foreword to the Information Security Policy

The current era is often referred to as the “information age”. We have seen a massive change in the way humans generate, store and exchange information. It has also profoundly altered the terms by which we interact with each other, not just as individuals, but also within and between institutions, societies and nations. We have accrued great benefits from this new era, but it brings with it profound challenges in the areas of security and privacy, which have been reflected in the growth of legislation around the globe concerning the holding of information.

As an education institution committed to both high quality teaching and research, Attenborough has an ethical, legal and professional duty to ensure that the information it holds conforms to the principles of confidentiality, integrity and availability. We must ensure that the information we hold or are responsible for is safeguarded where necessary against inappropriate disclosure; is accurate, timely and attributable; and is available to those who should be able to access it.
The Information Security Policy below provides the framework by which we take account of these principles. Its primary purpose is to enable all Attenborough staff and pupils to understand both their legal *and* ethical responsibilities concerning information, and empower them to collect, use, store and distribute it in appropriate ways.
This policy is the cornerstone of Attenborough’s on-going commitment to enhance and clarify our information security procedures. It has my full support and I encourage all Attenborough staff to read it and abide by it in the course of their work.

MOD employees including Teachers and LEC are to ensure they have carried out the relative Information Security training, training is to be completed once every 3 years and reported to Army HQ through HQ DCYP.

For those staff who have access to sensitive personal information but who do not regularly use MoD IT system are to undertake:
‘Responsible for Information General User’ training which is mandatory once every 3 years, training can be done through the Civil Service Learning

For those staff that use DII on a regular basis are required to undertake:
The ‘Defence Information Management Passport: Information Matters v5.0’ training which is mandatory once every 3 years, training can be done through the Defence Learning Environment (through the Defence Gateway www.defencegateway.mod.uk) – Course code is: Info Matters.

(please note if you carry out the Defence Information Management Passport training you do NOT have to carry out the Responsible for Information training).

1 Introduction

The confidentiality, integrity and availability of information, in all its forms, are critical to the on-going functioning and good governance of Attenborough School. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for Attenborough School to recover.
This information security policy outlines Attenborough School's approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the School's information systems. Supporting policies, codes of practice, procedures and guidelines provide further details.
Attenborough School is committed to a robust implementation of Information Security Management. It aims to ensure the appropriate confidentiality, integrity and availability of its data. The principles defined in this policy will be applied to all of the physical and electronic information assets for which the Attenborough School is responsible.
Attenborough School is specifically committed to preserving the confidentiality, integrity and availability of documentation and data supplied by, generated by and held on behalf of third parties pursuant to the carrying out of work agreed by contract in accordance with the requirements of data security standard ISO 27001.

1.1 Objectives

The objectives of this policy are to:

1. Provide a framework for establishing suitable levels of information security for all Attenborough School information systems (including but not limited to all Cloud environments commissioned or run by Attenborough School, computers, storage, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems. a. This explicitly includes any ISO27001-certified Information Security Management Systems the School may run.
b. The resources required to manage such systems will be made available
c. Continuous improvement of any ISMS will be undertaken in accordance with *Plan Do Check Act* principles

2. Make certain that users are aware of and comply with all current and relevant UK and EU legislation.

3. Provide the principles by which a safe and secure information systems working environment can be established for staff, pupils and any other authorised users.

4. Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.

5. Protect Attenborough School from liability or damage through the misuse of its IT facilities.

6. Maintain research data and other confidential information provided by suppliers at a level of security commensurate with its classification, including upholding any legal and contractual requirements around information security.

7. Respond to changes in the context of the organisation as appropriate, initiating a cycle of continuous improvement.

1.2 Scope

This policy is applicable to, and will be communicated to, all staff, pupils, other members of the School and third parties who interact with information held by the Attenborough School and the information systems used to store and process it.
This includes, but is not limited to: Cloud systems developed or commissioned by Attenborough School, any systems or data attached to the Attenborough School data or telephone networks, systems managed by Attenborough School, mobile devices used to connect to Attenborough School networks or hold Attenborough School data, data over which Attenborough School holds the

intellectual property rights, data over which Attenborough School is the data controller or data processor, electronic communications sent from the Attenborough School.

2 Policy

2.1 Information security principles

The following information security principles provide overarching governance for the security and management of information at Attenborough School.
1. Information should be classified according to an appropriate level of confidentiality, integrity and availability (see *Section 2.3. Information Classification*) and in accordance with relevant legislative, regulatory and contractual requirements (see *Section 2.2. Legal and Regulatory Obligations*).

2. Staff with particular responsibilities for information (see *Section 3. Responsibilities*) must ensure the classification of that information; must handle that information in accordance with its classification level; and must abide by any contractual requirements, policies, procedures or systems for meeting those responsibilities.

3. All users covered by the scope of this policy (see *Section 1.2. Scope*) must handle information appropriately and in accordance with its classification level.

4. Information should be both secure and available to those with a legitimate need for access in accordance with its classification level. a. On this basis, access to information will be on the basis of *least privilege* and *need to know*.

5. Information will be protected against unauthorized access and processing in accordance with its classification level.

6. Breaches of this policy must be reported (see Sections *2.4. Compliance* and *2.5. Incident Handling*).

7. Information security provision and the policies that guide it will be regularly reviewed, including through the use of annual internal audits and penetration testing.

8. Any explicit Information Security Management Systems (ISMSs) run within the School will be appraised and adjusted through the principles of continuous improvement, as laid out in ISO27001 clause 10.

2.2 Legal & Regulatory Obligations

Attenborough School has a responsibility to abide by and adhere to all current UK and EU legislation as well as a variety of regulatory and contractual requirements.
A non-exhaustive summary of the legislation and regulatory and contractual obligations that contribute to the form and content of this policy is provided in *Appendix A*.

2.3 Compliance, Policy Awareness and Disciplinary Procedures

Any security breach of Attenborough School's information systems could lead to the possible loss of confidentiality, integrity and availability of personal or other confidential data stored on these information systems. The loss or breach of confidentiality of personal data is an infringement of the General Data Protection Regulation, contravenes Attenborough School's Data Protection Policy, and may result in criminal or civil action against Attenborough School.

The loss or breach of confidentiality of contractually assured information may result in the loss of business, financial penalties or criminal or civil action against Attenborough School. Therefore it is crucial that all users of the School's information systems adhere to the Information Security Policy and its supporting policies as well as the Information Classification Standards.
All current staff, pupils and other authorised users will be informed of the existence of this policy and the availability of supporting policies, codes of practice and guidelines.
Any security breach will be handled in accordance with all relevant School policies, including the *Conditions of Use of IT Facilities at the Attenborough School* and the appropriate disciplinary policies.

2.7 Incident Handling

If a member of the School (staff or student) is aware of an information security incident then they must report it to the Information Management and Technology Service Desk at ServiceDesk@modschools.org or telephone 00441980615166
Breaches of personal data will be reported to the Information Commissioner's Office by Attenborough School's Data Protection Officer.

2.8 Supporting Policies, Codes of Practice, Procedures and Guidelines

All staff, pupils and any third parties authorised to access Attenborough School's network or computing facilities are required to familiarise themselves with this policy and to adhere to it in the working environment.

2.9 Review and Development

This policy shall be reviewed by Attenborough and updated regularly to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.
Additional regulations may be created to cover specific areas.

3 Responsibilities

Members of Attenborough School:
All members of Attenborough School, Attenborough School associates, agency staff working for Attenborough School, third parties and collaborators on
Attenborough School projects will be users of Attenborough School information. This carries with it the responsibility to abide by this
policy and its principles and relevant legislation, supporting policies, procedures and guidance. No individual should be able to access information to which they do not have a legitimate access right. Notwithstanding systems in place to prevent this, no individual should knowingly contravene this policy, nor allow others to do so. To report policy contraventions, please see Section 2.5: Incident Handling
Data Controllers:
Many members of Attenborough School will have specific or overarching responsibilities for preserving the
confidentiality, integrity and availability of information. These include:
Principal Investigators / Project administrators:
Responsible for the security of information produced, provided or held in the course of carrying out research, consultancy or knowledge transfer activities. This includes ensuring that data is appropriately stored, that the risks to data are appropriately understood and either mitigated or explicitly accepted, that the correct access rights have been put in place, with data only accessible to the right people, and ensuring there are appropriate backup, retention, disaster recovery and disposal mechanisms in place.
Heads of Departments, Divisions, Centres:
Responsible for the information systems (e.g. HR/ Registry/ Finance) both manual and electronic that support Attenborough School's work. Responsibilities as above (for Principal Investigators / Project administrators).
Departmental managers / Line managers:
Responsible for specific area of Attenborough School work, including all the supporting information and documentation
that may include working documents/ contracts/ staff or student information.
Head of Research Division:
Signs off Attenborough School research contracts and is responsible for providing the assurance that any mandated
security measures for research data are met.
School Secretary:
Responsible for Attenborough School compliance with the general Data Protection regulation
Records Manager / Data Protection Officer:

Responsible for Attenborough School's Data Protection Policy, data protection and records retention issues. Breach
reporting to ICO

IMT and devolved School IT teams:
Responsible for ensuring that the provision of Attenborough School's IT infrastructure is consistent with the demands
of this policy and current good practice.

Head of Security:
Responsible for physical aspects of security and will provide specialist advice throughout the Attenborough School on
physical security issues.

Information Security Team:
Responsible for this and subsequent information security policies and will provide specialist advice throughout the School on information security issues.

Information Security Advisory Board:
Responsible for the advising on and recommending information security policies to the Information Technology Committee, assessing information security risks, identifying and implementing controls to risks.

Information Technology Committee:
Responsible for approving information security policies.

4 Appendix A: Summary of relevant legislation

4.1 The Computer Misuse Act 1990

Defines offences in relation to the misuse of computers as:
1. Unauthorised access to computer material.
2. Unauthorised access with intent to commit or facilitate commission of further offences.
3. Unauthorised modification of computer material.

4.2 The Freedom of Information Act 2000

The Freedom of Information Act 2000 (FOIA2000) is a general right of public access to all types of recorded information held by public authorities in order to promote a culture of openness and accountability.

4.3 Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 regulates the powers of public bodies to carry out surveillance and investigation. It covers the interception and use of communications data and can be invoked in the cases of national security, and for the purposes of detecting crime, preventing disorder, public safety and protecting public health.

4.4 Defamation Act 1996

"Defamation is a faAttenborough School accusation of an offence or a malicious misrepresentation of someone's words or actions. The defamation laws exist to protect a person or an organisation's reputation from harm".

4.5 Obscene Publications Act 1959 and 1964

The law makes it an offence to publish, whether for gain or not, any content whose effect will tend to "deprave and corrupt" those likely to read, see or hear the matter contained or embodied in it. This could include images of extreme sexual activity such as bestiality, necrophilia, rape or torture.

4.6 Protection of Children Act 1978, Criminal Justice Act 1988, Criminal Justice and Immigration Act 2008

The Protection of Children Act 1978 *prevents the exploitation of children by making indecent photographs of them and penalises the distribution and showing of such indecent photographs.*
Organisations must take appropriate steps to prevent such illegal activities by their workers using their digital systems and networks.
The definition of 'photographs' include data stored on a computer disc or by other electronic means which is capable of conversion into an image.
It is an offence for a person to […] distribute or show such indecent photographs; or to possess such indecent photographs, with a view to their being distributed or shown by himself or others.

Section 160 of the Criminal Justice Act 1988 made the simple possession of indecent photographs of children an offence. Making an indecent image of a child is a serious arrestable offence carrying a maximum sentence of 10 years imprisonment. Note: The term "make" includes downloading images from the Internet and storing or printing them out.

4.7 Terrorism Act 2006

The Terrorism Act 2006 makes it an offence to write, publish or circulate any material that could be seen by any one or more of the persons to whom it has or may become available, as a direct or indirect encouragement or other inducement to the commission, preparation or instigation of acts of terrorism.

It also prohibits the writing, publication or circulation of information which is likely to be useful to any one or more persons in the commission or preparation of terrorist acts or is in a form or context in which it is likely to be understood by any one or more of those persons as being wholly or mainly for the purpose of being so useful.

In addition, it prohibits the glorification of the commission or preparation (whether in the past, in the future or generally) of terrorist acts or such offences; and the suggestion that what is being glorified is being glorified as conduct that should be emulated in existing circumstances.

4.8 Counter-Terrorism and Security Act 2015 – Statutory Guidance

The statutory guidance accompanying the Counter-Terrorism and Security Act 2015 (Prevent duty guidance for higher education institutions in England and Wales https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445916/Prevent_Duty_Guidance For Higher Education England Wales.pdf) requires Attenborough School to have “due regard to the need to prevent people from being drawn into terrorism.” The Act imposes certain duties under the *Prevent* programme, which is aimed at responding to “the ideological challenge we face from terrorism and aspects of extremism, and the threat we face from those who promote these views.” The Prevent programme also aims to provide “practical help to prevent people from being drawn into terrorism and ensure they are given appropriate advice and support”. Attenborough School must balance its existing legal commitments to uphold academic freedom and (under the Education (No. 2) Act 1986) freedom of speech within the law against the new Prevent duty, and seek to ensure that its IT facilities are not used to draw people into terrorism.

4.9 General Data Protection Regulation

The GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK’s decision to leave the EU will not affect implementation of the GDPR. The GDPR reinforces and extends data subjects’ rights as laid out in the Data Protection Act (1998), and provides additional stipulations around accountability and governance, breach notification and transfer of data. It also extends the maximum penalties liable due to a data breach, from £500,000 to 4% global turnover. The GDPR requires Attenborough School to maintain an Information Asset Register, to ensure where personal data is voluntarily gathered people are required to explicitly opt in, and can also easily opt out. It requires data breaches to be reported to the Information Commissioner’s Office within 72hrs of Attenborough School becoming aware of their existence.