



## INFORMATION SECURITY POLICY

The General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The Centre is dedicated to ensure the security of all information that it holds and implements the highest standards of information security in order to achieve this. This document sets out the measures taken by The Centre to achieve this, including to: -

- protect against potential breaches of confidentiality;
- ensure that all information assets and IT facilities are protected against damage, loss or misuse;
- support our Data Protection Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data; and
- increase awareness and understanding at The Centre of the requirements of information security and the responsibility to staff to protect the confidentiality and integrity of the information that they themselves handle.

### **Introduction**

Information Security can be defined as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.

Staff are referred to The Centre's Data Protection Policy, Data Breach Policy and Electronic Information and Communication Systems Policy for further information. These policies are also designed to protect personal data and can be found in Waterside Office or on our website [here](#). For the avoidance of doubt, the term 'mobile devices' used in this policy refers to any removable media or mobile device that can store data. This includes, but is not limited to, laptops, tablets, digital cameras, memory sticks and smartphones.

Staff should also refer to our Safeguarding policy and the current version of Keeping Children Safe in Education which can be found [here](#).

## **Scope**

The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of The Centre, in whatever media. This includes information held on computer systems, paper records, hand-held devices, and information transmitted orally.

This policy applies to all members of staff, including temporary staff, other contractors, volunteers, Governors and any and all third parties authorised to use the IT systems.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under The Centre's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with The Centre and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

## **General principles**

All data stored on our IT systems are to be classified appropriately (including, but not limited to, personal data, special category data and confidential information. Further details on the categories of data can be found in The Centre's Data Protection Policy and Record of Processing Activities). All data so classified must be handled appropriately in accordance with its classification.

Staff should discuss with the Business Manager the appropriate security arrangements for the type of information they access in the course of their work.

All data stored on our IT Systems and our paper records shall be available only to members of staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption.

All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by our Software Support or by such third party/parties as the Headteacher may authorise.

The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with the Headteacher unless expressly stated otherwise.

All staff have an obligation to report actual and potential data protection compliance failures to the Headteacher who shall investigate the breach. Any breach which is either known or suspected to involve personal data or special category data shall be reported to the Data Protection Officer (full details of the officer can be found in our Data Protection Policy).

### **Physical security and procedures**

Paper records and documents containing personal information, special category data, and confidential information shall be positioned in a way to avoid them being viewed by people passing by as much as possible, e.g., through windows. At the end of the working day, or when you leave your desk unoccupied, all paper documents shall be securely locked away to avoid unauthorised access.

Available storage rooms, locked cabinets, and other storage systems with locks shall be used to store paper records when not in use.

Paper documents containing confidential personal information should not be left on office and classroom desks, on staffroom tables, or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained. You should take particular care if documents have to be taken out of school.

The physical security of buildings and storage systems shall be reviewed on a regular basis. If you find the security to be insufficient, you must inform the Headteacher as soon as possible. Increased risks of vandalism and or burglary shall be taken into account when assessing the level of security required.

The Centre carry out regular checks of the buildings and storage systems to ensure they are maintained to a high standard.

The Centre close The Centre gates during certain hours to prevent unauthorised access to the building. An alarm system is set nightly.

Visitors are required to sign in at the reception, accompanied at all times by a member of staff and never be left alone in areas where they could have access to confidential information.

All physical documents containing confidential data are either shredded on site or for bulk items put in confidential waste bags and sealed and disposed of through a contract we have with RBC.

### **Computers and IT Responsibilities of the ICT Support Provider**

The ICT Support Provider shall be responsible for the following:

- a) ensuring that all IT Systems are assessed and deemed suitable for compliance with The Centre's security requirements;
- b) ensuring that IT Security standards within The Centre are effectively implemented and regularly reviewed, working in consultation with The Centre's management, and reporting the outcome of such reviews to The Centre's management;
- c) ensuring that all members of staff are kept aware of this policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force, including, but not limited to, the UK GDPR and the Computer Misuse Act 1990.

Furthermore, the ICT Support Provider shall be responsible for the following:

- a) assisting all members of staff in understanding and complying with this policy;
- b) providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems;
- c) ensuring that all members of staff are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities, and any special security requirements;
- d) receiving and handling all reports relating to IT Security matters and taking appropriate action in response [including, in the event that any reports relate to personal data, informing the Data Protection Officer];
- e) taking proactive action, where possible, to establish and implement IT security procedures and raise awareness among members of staff;
- f) monitoring all IT security within The Centre and taking all necessary action to implement this policy and any changes made to this policy in the future; and
- g) ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

### **Responsibilities – Members of staff**

All members of staff must comply with all relevant parts of this policy at all times when using the IT Systems.

Computers and other electronic devices should be locked when not in use to minimise the accidental loss or disclosure.

You must immediately inform the Headteacher of any and all security concerns relating to the IT Systems which could or has led to a data breach as set out in the Data Breach Policy.

Any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems shall be reported to the Headteacher immediately.

You are not entitled to install any software of your own without the approval of the Software Support Company. Any software belonging to you must be approved by them and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.

Prior to installation of any software onto the IT Systems, you must obtain written permission by the Software Support Company. This permission must clearly state which software you may install, and onto which computer(s) or device(s) it may be installed.

Prior to any usage of physical media (e.g., USB memory sticks or disks of any kind) for transferring files, you must make sure the physical media is virus-scanned. The Headteacher's approval must be obtained prior to transferring of files using cloud storage systems.

If you detect any virus this must be reported immediately to the Headteacher (this rule shall apply even where the anti-virus software automatically fixes the problem).

### **Access security**

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

The Centre has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to protect The Centre's network. The Centre also teach individuals about e-safety as part of induction to ensure everyone is aware of how to protect The Centre's network and themselves.

All IT Systems (in particular mobile devices) shall be protected with a secure password or passcode, or such other form of secure log-in system as approved by the IT Department. Biometric log-in methods can only be used if approved by the IT Department.

All passwords must, where the software, computer, or device allows:

- a) be at least 12 characters long including both numbers a capital letter and a special character and change is prompted by system.
- b) be changed on a regular basis [and at least every 180 days];
- c) cannot be the same as the previous 10 passwords you have used;
- d) not be obvious or easily guessed (e.g., birthdays or other memorable dates, memorable names, events, or places etc.)

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Management Team who will liaise with the SMT members as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under The Centre's Disciplinary Policy and Procedure.

If you forget your password, you should notify the current Software support Provider to have your access to the IT Systems restored. You must set up a new password immediately upon the restoration of access to the IT Systems.

You should not write down passwords if it is possible to remember them. If necessary, you may write down passwords provided that you store them securely (e.g., in a locked drawer or in a secure password database). Passwords should never be left on display for others to see.

Computers and other electronical devices with displays and user input devices (e.g., mouse, keyboard, touchscreen etc.) shall be protected with a screen lock that will activate after a period of inactivity.

All mobile devices provided by The Centre, shall be set to lock, sleep, or similar, after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake or similar.

Staff should be aware that if they fail to log off and leave their terminals unattended, they may be held responsible for another user's activities on their terminal in breach of this policy, The Centre's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

### **Data security**

Personal data sent over The Centre network will be encrypted or otherwise secured.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from SMT who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins. Where consent is given all files and data should always be virus checked before they are downloaded onto The Centre's systems.

You may connect your own devices (including, but not limited to, laptops, tablets, and smartphones) to The Centre's Wi-Fi provided that you follow SMT's requirements and instructions governing this use. All usage of your own device(s) whilst connected to The Centre's network or any other part of the IT Systems is subject to all relevant School Policies (including,

but not limited to, this policy). SMT may at any time request the immediate disconnection of any such devices without notice.

### **Electronic storage of data**

All portable data, and in particular personal data, should be stored on encrypted drives using methods recommended by SMT.

All data stored electronically on physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.

You should not store any personal data on any mobile device, whether such device belongs to The Centre or otherwise without prior written approval of SMT. You should delete data copied onto any of these devices as soon as possible and make sure it is stored on The Centre's computer network in order for it to be backed up.

All Electronic files to be stored on drives that are backed up by our Software Support provider. These are drives S drive, shared drive, Curriculum Drive or your own document drive z drive. **Not the c drive or desktop as this is local to your machine and not backed up or as secure.** If you are unsure then please see either Business Manager or ICT support engineer to discuss.

All electronic data must be securely backed up by the end of the each working day and is done by our Software Support provider.

### **Home working**

You should not take confidential or other information home without prior permission of the Head and only do so where satisfied appropriate technical and practical measures are in place within your home to maintain the continued security and confidentiality of that information.

When you have been given permission to take confidential or other information home, you must ensure that:

- a) the information is kept in a secure and locked environment where it cannot be accessed by family members or visitors; and

- b) all confidential material that requires disposal is brought back to the Centre to be shredded confidentially or, in the case of electronical material, securely destroyed, as soon as any need for its retention has passed.
- c) Sign a specific home working agreement giving you specific permission to take information home for a specific purpose or length of time. Then returned to be securely destroyed in accordance with Data retention policy when no longer in use.

### **Communications, transfer, internet and email use**

When using The Centre's IT Systems, you are subject to and must comply with The Centre's Electronic Information and Communication Systems Policy.

The Centre work to ensure the systems do protect pupils and staff and are reviewed and improved regularly.

If staff or pupils discover unsuitable sites or any material which would be unsuitable, this should be reported to the Head.

Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee and The Centre cannot accept liability for the material accessed or its consequence.

All personal information, and in particular sensitive personal information and confidential information should be encrypted before being sent by email, or sent by tracked DX (document exchange) or recorded delivery. You may not send such information by fax unless you can be sure that it will not be inappropriately intercepted at the recipient fax machine.

Postal, DX, fax and email addresses and numbers should be checked and verified before you send information to them. In particular you should take extra care with email addresses where auto-complete features may have inserted incorrect addresses.

You should be careful about maintaining confidentiality when speaking in public places.

You should make sure to mark confidential information 'confidential' and circulate this information only to those who need to know the information in the course of their work for The Centre.

Personal or confidential information should not be removed from The Centre without prior permission from the Head except where the removal is temporary and necessary. When such permission is given, you must take all reasonable steps to ensure that the integrity of the information and the confidentiality are maintained. You must ensure that the information is:

- a) not transported in see-through or other un-secured bags or cases;
- b) not read in public places (e.g., waiting rooms, cafes, trains, etc.); and

- c) not left unattended or in any place where it is at risk (e.g., in car boots, cafes, etc.)

### **Reporting security breaches**

All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the Head. All members of staff have an obligation to report actual or potential data protection compliance failures.

When receiving a question or notification of a breach, the Head shall immediately assess the issue, including but not limited to, the level of risk associated with the issue, and shall take all steps necessary to respond to the issue.

Members of staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the Head who will consult with the Data Protection Officer. Any attempt to resolve an IT security breach by a member of staff must be under the instruction of, and with the express permission of, the Data Protection Officer.

Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to the Head in the first instance.

All IT security breaches shall be fully documented.

Full details on how to notify of data breaches are set out in the Data Breach Policy.

**Related Policies:** Staff should refer to the following policies that are related to this information security policy: -

- Electronic Information and Communication Systems Policy;
- Data Breach policy;
- Data Protection Policy.
- Appendix 1 Cyber Security Policy

**Policy Agreed: Oct 2025**

**Policy to be Reviewed every 2 years by Finance Committee**

**Next review Oct 2027**

## Appendix 1

### **Introduction**

Cyber security has been identified as a risk for the Centre and every employee needs to contribute to ensure data security.

For more information please refer to the National Cyber Security Centre Guidance for Schools, [here](#).

The Centre has invested in technical cyber security measures but we also need our employees to be vigilant and to act to protect the Centre IT systems.

The Headteacher is responsible for cyber security within the Centre.

If you are an employee, you may be liable to disciplinary action if you breach this policy.

### **What is Cyber-Crime?**

Cyber-crime is simply a criminal activity carried out using computers or the internet including hacking, phishing, malware, viruses or ransom attacks.

The following are all potential consequences of cyber-crime which could affect an individual and/or individuals:

- Cost – The global cost of all forms of online crime is estimated to be in excess of £300 billion. We may be fined up to £17.5 million or 4% of the total worldwide annual turnover if we fail to protect our data.
- Confidentiality and data protection - Protecting individuals' confidential information and all forms of personal data is one of the most essential requirements our school. The risk to confidential information and personal data is the biggest of all threats from cyber-crime.
- Potential for regulatory breach – We have various regulatory duties which we could unintentionally breach through falling victim to cyber-crime or a cyber-attack. Loss of personal data can lead to claims for damages by the individuals concerned and/or significant fines from the Information Commissioners Office (ICO).
- Reputational damage – A cyber security incident can have a major impact on our reputation, particularly if it involves the loss of confidential information, personal data and/or is reported in the media. Protecting our reputation is of utmost importance.
- Business interruption – Some forms of cyber-attack could render key systems (for instance servers including email servers, cloud computing services or our website) unavailable. This

would have a major impact on delivering lessons and delivering our services. It may be necessary in such cases to invoke our Business Continuity Plan. The Business Manager is responsible for making that decision and communicating with IT.

- Structural and financial instability – The financial losses flowing from online crime may cause or contribute to financial difficulty.

### **Cyber-Crime Prevention**

Given the seriousness of the consequences noted above, it is important for the Centre to take preventative measures and for staff to follow the guidance within this policy.

This cyber-crime policy sets out the systems we have in place to mitigate the risk of cyber-crime. We can provide further details of other aspects of the Centre/Trust risk assessment process upon request.

The Centre have put in place a number of systems and controls to mitigate the risk of falling victim to cyber-crime. These include technology solutions as well as controls and guidance for staff.

### **Technology Solutions**

The Centre have implemented the following technical measures to protect against cyber-crime:

- (i) firewalls;
- (ii) anti-virus software;
- (iii) anti-spam software;
- (iv) auto or real-time updates on our systems and applications;
- (v) URL filtering;
- (vi) secure data backup;
- (vii) encryption;
- (viii) deleting or disabling unused/unnecessary user accounts;
- (ix) deleting or disabling unused/unnecessary software;
- (x) using strong passwords; and
- (xi) disabling auto-run features

## Controls and Guidance for Staff

- All staff must follow the policies related to cyber-crime and cyber security as listed in this policy.
- All staff will be provided with training at induction and refresher training as appropriate; when there is a change to the law, regulation or policy; where significant new threats are identified and in the event of an incident affecting the Centre or any third parties with whom we share data.
- It may be appropriate in some instances to limit the number of people involved or who have access to information on a matter to ensure the security of the data involved. This can be part achieved through IT security measures. We may implement other controls that are more practical in nature, e.g.:
  - Physically ringfencing the individuals or teams working on a matter;
  - Taking steps to ensure our system for opening, distributing and/or scanning incoming correspondence (by post, email or otherwise) does not allow or inadvertent sharing of confidential information;
  - Getting a signed confidentiality agreement from each staff member;
  - Disposing of confidential documents securely;
  - Having a clear desk policy;
  - Discouraging staff from reading confidential papers or discussing sensitive matters in public.

Due diligence – we may conduct due diligence on the cyber security controls and cyber-crime prevention measures that other parties with whom we share information.

- 
- All staff must:
  - Choose strong passwords (the Centre's IT team advises that a strong password contains Capitals, numbers and a special character and be at least 12 digits long.
  - keep passwords secret;
  - never reuse a password;

- never allow any other person to access the Centre's systems using your login details;
- not turn off or attempt to circumvent any security measures (antivirus software, firewalls, web filtering, encryption, automatic updates etc.) that the IT team have installed on their computer, phone or network or the Centre IT systems;
- report any security breach, suspicious activity or mistake made that may cause a cyber security breach, to Business Manager as soon as practicable from the time of the discovery or occurrence. If your concern relates to a data protection breach you must follow our Data Breach Policy;
- only access work systems using computers or phones that the Centre owns. Staff may only connect personal devices to the Wi-Fi provided with permission from Headteacher.
- not install software onto your Centre computer or phone. All software requests should be made to the Business Manager; and
- avoid clicking on links to unknown websites, downloading large files or accessing inappropriate content using Centre equipment and/or networks.

The Centre considers the following actions to be a misuse of its IT systems or resources:

- any malicious or illegal action carried out against the Centre or using the Centre's systems;
- accessing inappropriate, adult or illegal content within Centre premises or using Centre equipment;
- excessive personal use of Centre's IT systems during working hours;
- removing data or equipment from Centre premises or systems without permission, or in circumstances prohibited by this policy;
- using Centre equipment in a way prohibited by this policy;
- circumventing technical cyber security measures implemented by the Centre's IT team; and
- failing to report a mistake or cyber security breach.

### **Cyber-Crime Incident Management Plan**

The incident management plan consists of four main stages:

- (i) *Containment and recovery:* To include investigating the breach, utilising appropriate staff to mitigate damage and where possible, to recover any data lost. We will notify our insurers as soon as reasonably practicable of any circumstances that may give rise to claim under relevant insurance policies. We will also assess whether it is necessary to invoke our business continuity plan.
- (ii) *Assessment of the ongoing risk:* To include confirming what happened, what data has been affected and whether the relevant data was protected. The nature and sensitivity of the data should also be confirmed and any consequences of the breach/attack identified.
- (iii) *Notification:* To consider whether the cyber-attack needs to be reported to regulators (for example, the ICO and National Crime Agency) and/or colleagues/parents as appropriate.
- (iv) *Evaluation and response:* To evaluate future threats to data security and to consider any improvements that can be made.

Where it is apparent that a cyber security incident involves a personal data breach, the Centre will invoke their Data Breach Policy rather than follow out the process above.